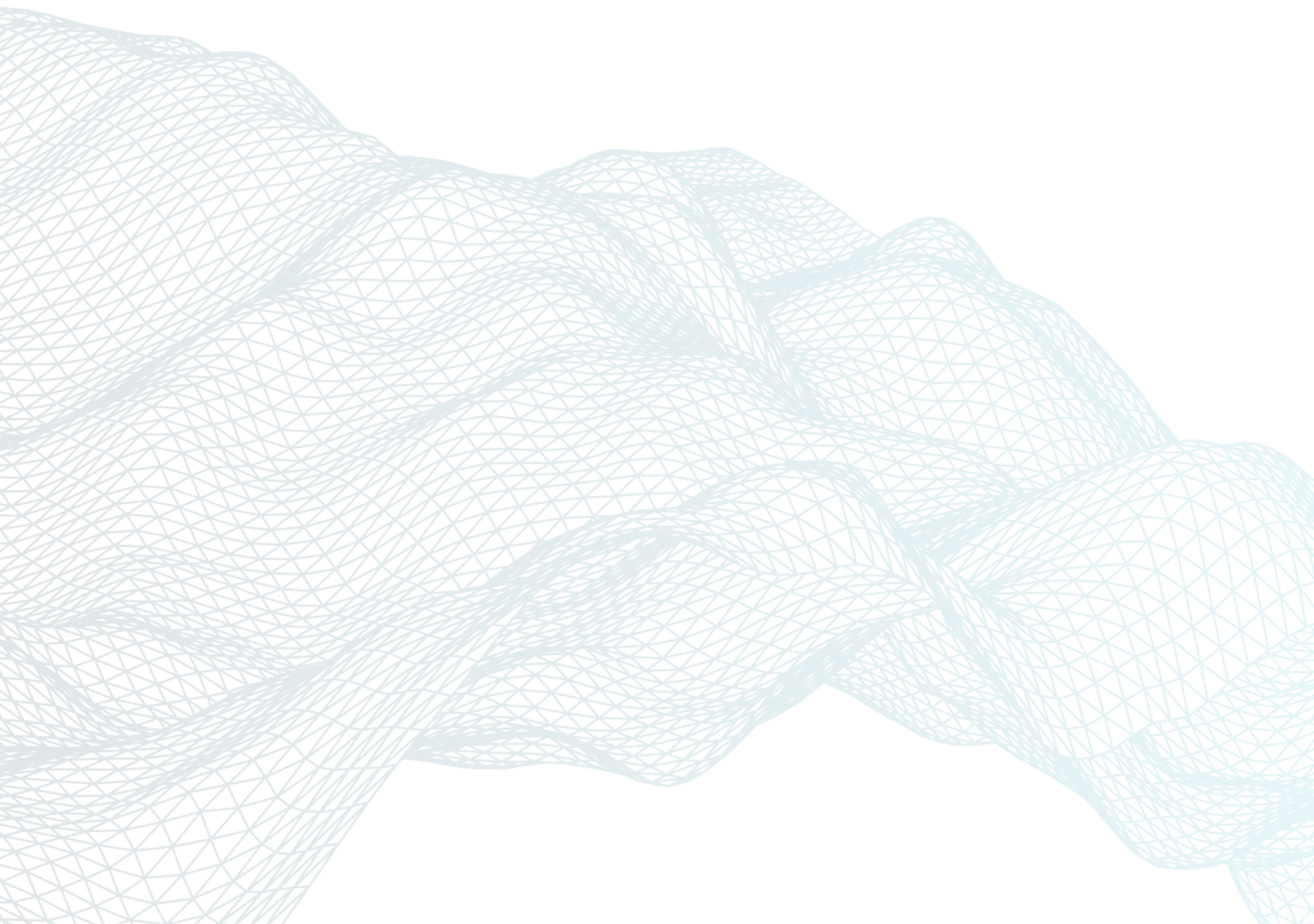


2021 eSENTIRE RANSOMWARE REPORT

---

# **Dissecting Today's Ransomware Ecosystem**

Ransomware-As-A-Service, Targeted Intrusions  
and Opportunistic Attacks



---

# Executive Summary

Cybercrime as we know it has changed.

What was once a world where petty criminals would compromise systems to snatch email addresses in order to peddle spam, assemble armies of botnets, and pilfer credit card numbers, has grown into a lucrative and highly profitable underground economy. Ransomware - malicious software designed to make a victim's data inaccessible until a ransom is paid has been a key to this evolution, allowing attackers to ratchet up payment demands to multi-million-dollar sums. And this doesn't include operational downtime costs, brand reputation value, and loss of consumer trust.

Ransomware has been a significant threat to organizations for years. What started as an opportunistic, automated attack against a single computer has evolved into a new business model for thieves. Instead of encrypting the data of a single computer system to hold for ransom, thieves instead now use this access as a persistent beachhead into organizations, leveraging it to spread as far and wide as they can before deploying ransomware, maximizing impact and devastation to extract maximum payout. This monetization model continues to develop, limited only by the creativity and callousness of those performing ransomware attacks.

Successful ransomware threat actors are sophisticated and savvy, their operations organized and well-run. Today's ransomware operators resemble enterprise organizations. Role specialization has afforded cybercrime groups the opportunity to procure specific services to expand both reach and velocity of ransomware campaigns, craft lures using industry-specific terminology, and execute every stage of a successful ransomware attack to maximize their return.

These advancements synthesize to make ransomware attacks a top-level risk to enterprise organizations. Ransomware has become a topic of discussion in executive suites around the world as organizations grapple with the magnitude and impact of this risk. With successful attacks unfolding in mere hours from initial access to data exfiltration and deployment of ransomware, CISOs need to re-evaluate their security program, posture, and controls against the backdrop of the heightened risk organizations face from today's threat actors. Security Operations groups also need up-to-the-minute threat detection capabilities and response playbooks to fully respond and remediate these attacks.

In this report, eSentire's Threat Response Unit (TRU) experts delve into the emergence of Ransomware-as-a-Service and discuss how criminals use this business model to perform both opportunistic and targeted attacks against victim organizations. We will share case studies along with our observations on the most popular initial access techniques used by these groups using real attacks. And finally, we will provide a set of actionable security takeaways that can be utilized to combat ransomware threats going forward.

---

# Key Takeaways

- Emergence of Ransomware-as-a-Service (RaaS) model has led to exponential growth in new ransomware groups. With this growth comes increased demand for extortion targets.
- What are generally considered opportunistic threats have risen to meet the demand, creating multiple entry points for ransomware that need to be defended.
- Commodity malware, credentials and exploits can be leveraged for gaining a foothold into organizations. This foothold can be monetized by selling access to or deploying ransomware.
- Former banking malware has evolved to aid in high-value target selection or specialize in consistent delivery into networks.
- Social engineering techniques dominate malicious code delivery. Email remains the most commonly detected vector, but web drive-by attacks are increasing in prevalence.
- Remote exploits such as ProxyLogon and use of stolen credentials devices is less common, but often highly impactful – especially when multi-factor authentication is not in use.
- Threat actors employ up to three additional leverage points, in addition to file encryption, to maximize extortion pressure on victims.
- As defenders, the need to identify and stop attacks as soon as possible has never been more important. Doing so successfully requires a combination of network hardening measures and robust detection and response capabilities.

## Methodology:

eSentire Threat Intelligence used data gathered from proprietary network and host-based detection sensors distributed globally across multiple industries. Raw data was normalized and aggregated using automated machine-based processing methods. Processed data was reviewed by a visual data analyst applying quantitative analysis methods. Quantitative intelligence analysis results were further processed by a qualitative intelligence analyst resulting in a written analytical product.

# Introduction

Opportunistic attacks have long been considered a “lesser evil” in business security priorities. Spam mail and unusual or suspicious websites are often regarded as minor annoyances and seen as an accepted risk of doing business on the internet. Starting in 2019, these perceived annoyances have served as footholds into organizations that open the door for intrusion specialists to manually circumvent defenses in preparation for ransomware deployment. The following report details the numerous opportunistic attack vectors that modern ransomware groups leverage through a versatile array of opportunity providers.

Ransomware-as-a-Service offerings have demonstrated an exponential increase in the past four years (Figure 1). Peering behind the scenes into the cybercrime marketplace where these shadow enterprises evolve gives insight into what is driving this exponential increase and why it is important to start taking apparent annoyances (like spam mail and strange websites) seriously. In short, the exponential increase is driven by role differentiation, in which different types of criminal specialists can focus on perfecting and developing their specific role in long-term intrusion campaigns by working together. Like the industrial period of the 20th century, in which the assembly line paradigm yielded highly efficient factories, a cooperative cybercrime marketplace lends greater efficiencies to the production of ransomware intrusions.

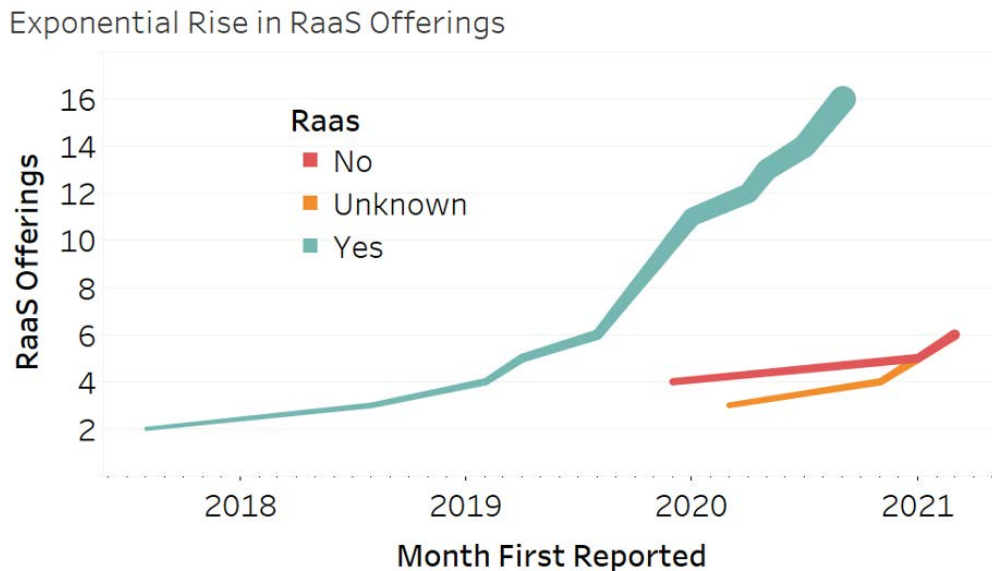


Figure 1: First observed activity of confirmed RaaS offerings



# 2021 Ransomware Threat Landscape

Prior to 2018, most financially motivated cyber-attacks were broken into two types: opportunistic attacks and targeted attacks, with opportunistic attacks being a numbers game (as in spam and scams) and targeted attacks more resembling a physical heist – in which particular assets are known about and targeted in a focused intrusion. As the cybercrime marketplace has matured, threat actors specializing in these two ends of the attack spectrum have found a class of integrated business models that maximizes advantages of each attack method and minimizes the disadvantages. Ransomware operations provide a reliable way to monetize intrusions, creating a demand chain in which intrusion specialists transact with opportunistic campaign operators.

The ransomware intrusion model can be generalized as a filtering system that acts to funnel opportunistic attacks into targeted ransomware intrusions (Figure 2). Opportunistic campaigns distribute foothold malware, such as trojans. Only a small subset of these attacks will yield successful delivery of their foothold payloads. However, their success signals an environment vulnerable to compromise. The provided foothold is then leveraged for intrusion actions (such as credential theft and lateral movement). If defenses can be overcome through intrusion actions, ransomware is deployed. Note that at each step of the model, victims are filtered to only the most susceptible, thus intrusion resources aren't wasted on well-defended environments with a low probability of success.



Figure 2: Target funnelling model by which opportunistic attacks become targeted attacks

# Gaining The Foothold: Opportunistic Malware Attacks

Opportunistic attacks that are known to be associated with ransomware were observed in high volumes throughout 2020, utilizing two primary initial access paths: email and web browsing (Figure 3). As stated previously, the objective of opportunistic malware is to gain a foothold in organizations and conduct a value assessment in preparation for intrusion specialists to carry out ransomware deployment. These cases rarely escalated to follow-on intrusion actions as a result of rapid identification and response by eSentire's 24/7 Security Operations Center.

Commodity malware and ransomware exhibit promiscuous relationships (Figure 4). For example, IcedID has been observed leading to DoppelPaymer, Sodinokibi, Egregor, RansomEXX, and Maze ransomware indicating its success as an initial access vector. Egregor has the most promiscuous ties with commodity malware, leveraging Qakbot, IcedID, SilentNight, and GootLoader to gain footholds into enterprise organizations. These footholds are in turn driven by mail distribution campaigns (as in Shathak, Emotet, and Zloader) and SEO redirection campaigns (as with GootLoader).

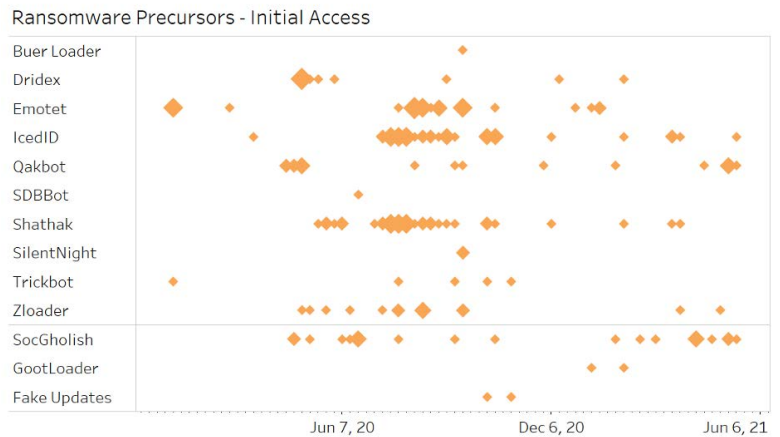


Figure 3: Ransomware precursors intercepted by eSentire.

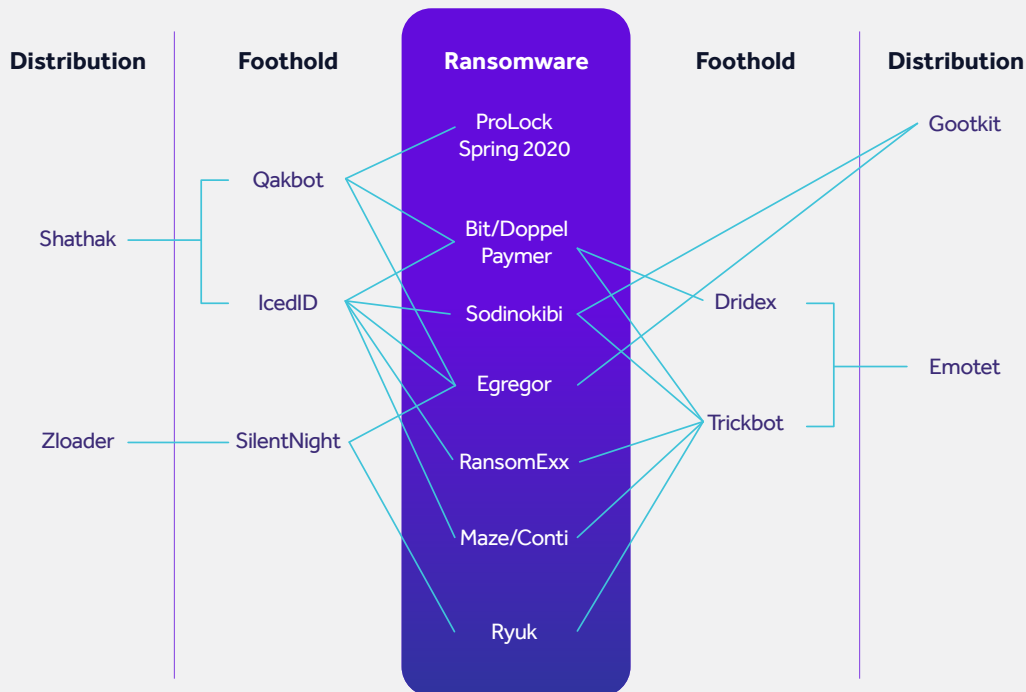


Figure 4: Promiscuous nature of relationships between email-based malware and ransomware

# Email-based attacks

Notable Examples: Emotet, Trickbot, Qakbot, IcedID, Zloader

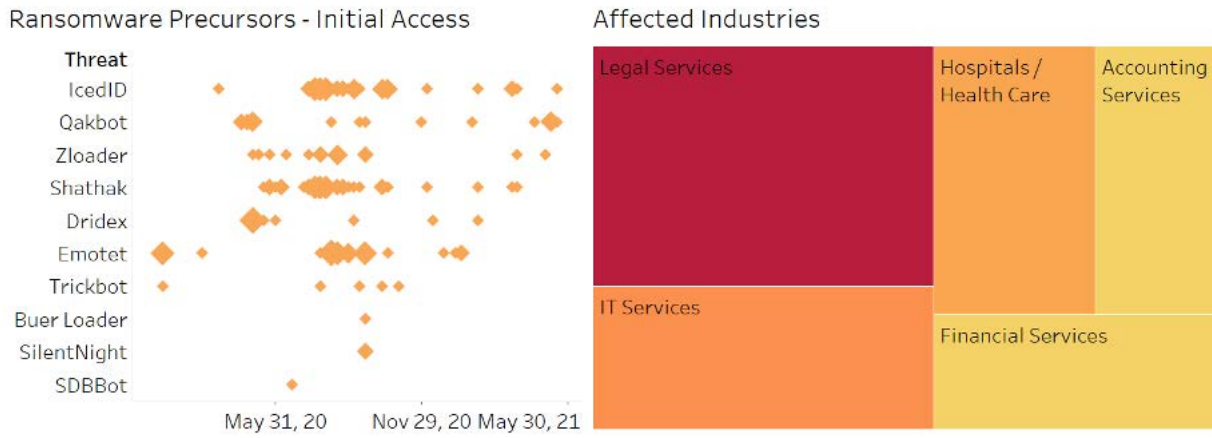


Figure 5: Email-based attack vector timeline and common industry targets

Throughout Spring and Summer of 2020, email-based attacks accounted for over 95% of ransomware affiliated threats tracked by eSentire’s Threat Response Unit (TRU), dominated largely by Shathak and Emotet spam campaigns (Figure 5). From Fall 2020 to Spring 2021, email-based attacks account for only 50% of ransomware-associated threats. Email-based attacks occur when a bad actor sends malicious attachments to an extensive list of victims. The lures used in such campaigns often target business professionals over private users. Popular business lures include payment invoices and legal threats, but more opportunistic lures including topics such as COVID-19, timely holiday themes, and tax and shipping documents – are still successful in enterprise environments.

# Case Study: Qakbot Leads to Cobalt Strike Deployment

**When:** May 2021

**Who:** Retail Organization

## Key Takeaways

The incident escalated from an opportunistic attack to Cobalt Strike and intrusion actions in just over an hour, demonstrating the efficiency in which attackers can zero-in on footholds in high-value networks.

## What Happened

eSentire's SOC detected and contained Cobalt Strike activity originating from a customer's endpoint. Root cause analysis revealed Cobalt Strike was deployed through Qakbot malware sometime earlier. eSentire's TRU team addressed detection gaps and conducted retro-hunts for IoAs and IoCs across all customers.

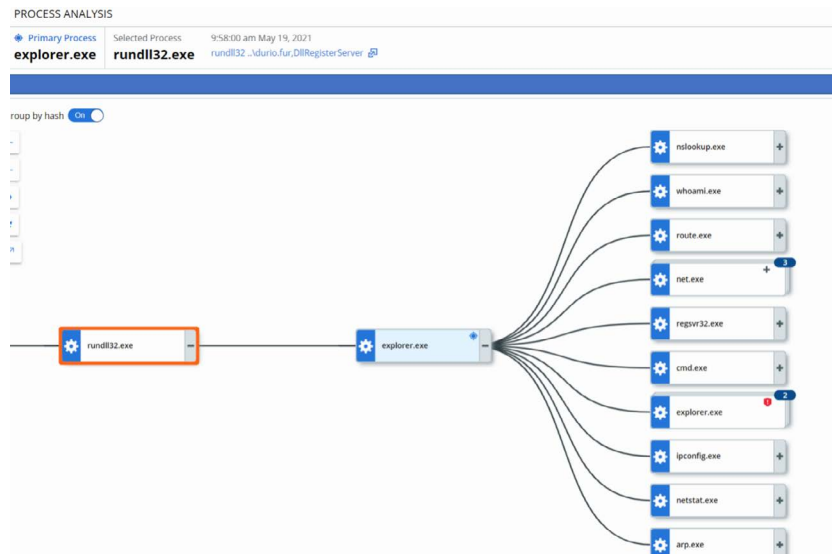


Figure 6: Recent Qakbot campaign profiling the network and victim immediately upon landing on the machine

The speed at which the Qakbot infection escalated is apparent when viewing the incident on a timeline:

- 10:00 AM - Victim opens malicious office document containing Qakbot payload
- 10:05 AM - Qakbot profiles the host and network, collecting data used to identify valuable organizations for intrusion actions. Information is communicated out through command-and-control channel.
- 10:20 AM - Cobalt Strike Beacon is deployed to the system
- 11:08 AM - Post exploitation tools such as Bloodhound and PowerSploit are observed
- While SOC awaited confirmation to isolate the system per the customer's policy, network disruption rules were placed on command-and-control channels. The attack did not progress beyond the initial deployment of post-exploitation tools.

## Link to Ransomware

External reports [1],[2],[3] have linked Qakbot to multiple ransomware groups, including ProLock [1], Egregor [2] and DoppelPaymer [3]. This attack was contained prior to ransomware deployment actions, but the deployment of CobaltStrike Beacon and subsequent attack tools is a strong indicator that follow-on ransomware was a goal.

1. <https://threatpost.com/prolock-ransomware-qakbot-trojan/155828/>
2. <https://www.recordedfuture.com/egregor-ransomware-attacks/>
3. <https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf>



# Web-Based Attacks

Notable Threats: Socgholish, Gootloader, FakeUpdates

## Ransomware Precursors - Initial Access



## Affected Industries

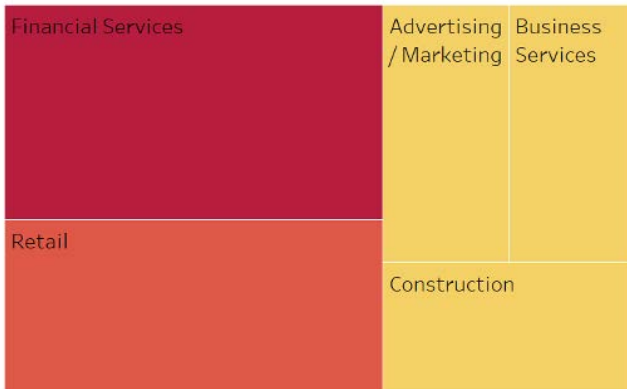


Figure 7: Impacted industries from web-based attacks

Web-based attacks have remained a contender for opportunistic initial access, maintaining consistent volumes through most of 2020 with a slight increase in 2021. They occur when a user is browsing the web and is socially engineered into downloading and executing malicious files. Two approaches to this attack are known vectors for ransomware. TRU has observed multiple Gootloader campaigns leveraging poisoned Google search results to lure victims onto attacker-controlled websites, where malware payload disguised as the search subject is presented. Gootloader has been associated with Revil and Egregor ransomware groups (Figure 8). The SocGholish threat leverages fake security warnings to coerce users into installing malware masquerading as browser updates (Figure 9). SocGholish has previously been associated with WastedLocker ransomware.

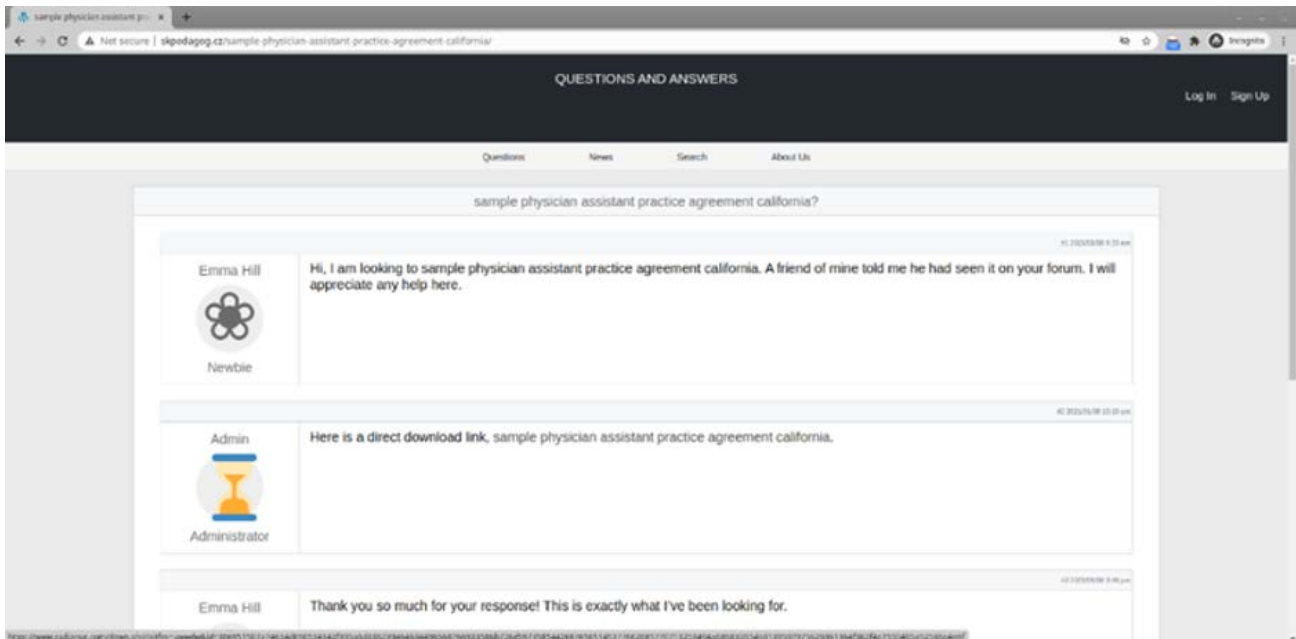


Figure 8: GootLoader. A fake forum pretending to offer the content user had just searched Google for

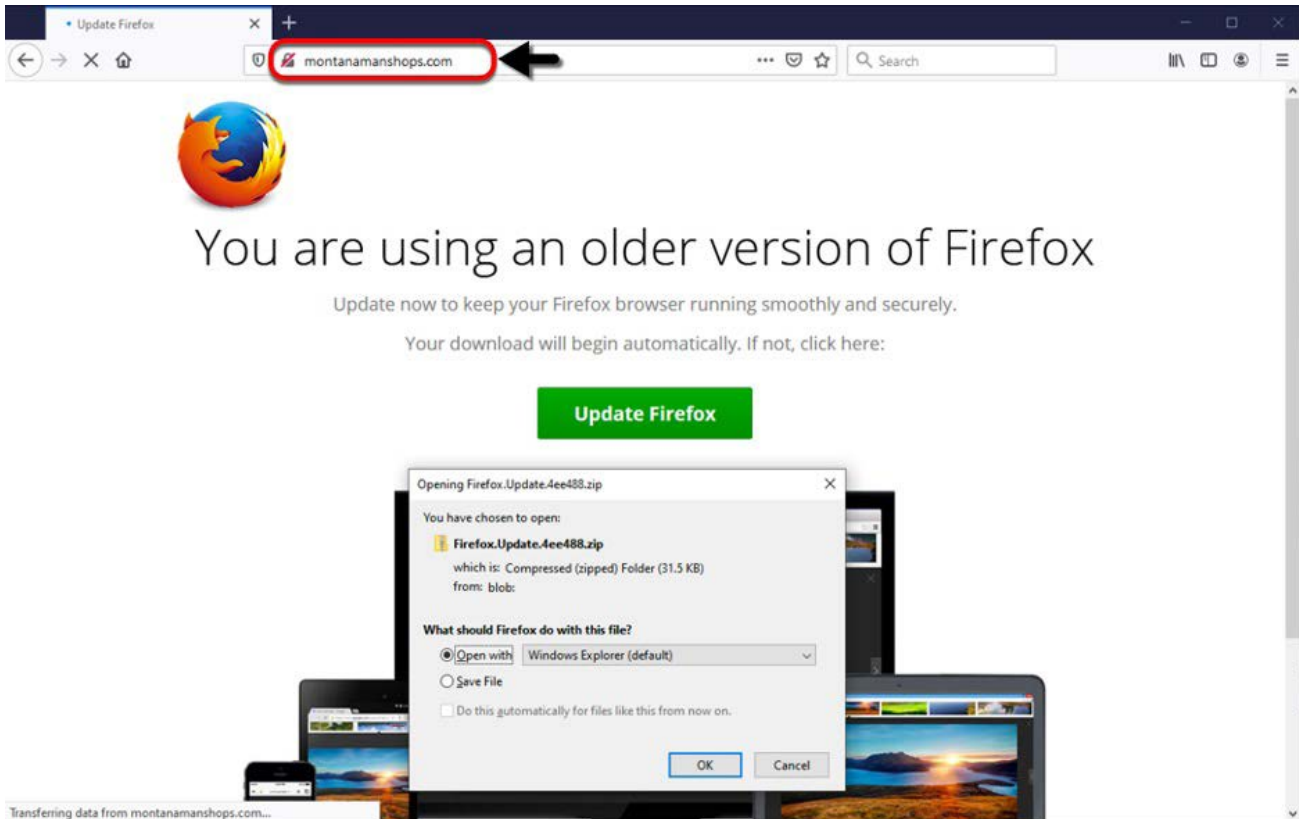


Figure 9: SocGhosh. A web-based attack using fake broser alerts to trick users into downloading a malicious payload [image credit: Brad Duncan]

## Case Study: FakeUpdates Campaign Linked to Ransomware

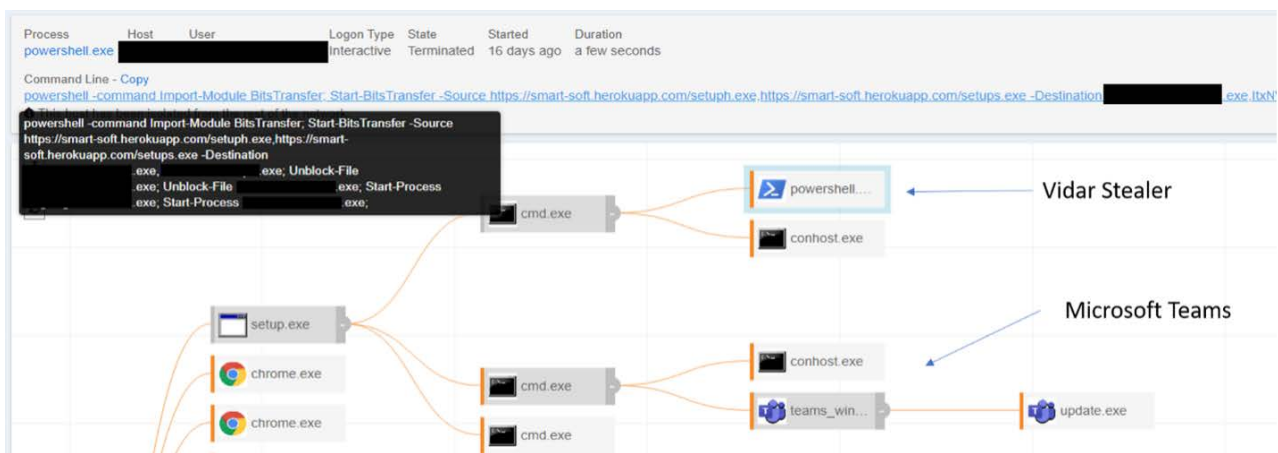


Figure 10: FakeUpdates infection chain

**When:** Fall 2020

**Who:** Manufacturing and eCommerce Organizations

## Key Takeaways

The popularity of collaboration software during the COVID-19 pandemic has soared as users transition to working from home. eSentire responded to a drive-by attack campaign impersonating popular virtual collaboration software Microsoft Teams to deliver information stealing malware. If allowed to remain undetected, this access was weaponized by ransomware actors according to an advisory by Microsoft.

## What Happened

In fall 2020 eSentire identified and contained information stealing malware (Vidar) across several customer environments. A root cause investigation revealed the victims had unintentionally executed malware masquerading as legitimate setup files for Microsoft Teams. These setup files were delivered by look-a-like websites for Microsoft hosted on the Heroku cloud platform. The attack was identified and contained by SOC prior to any follow-on actions.

## Links to Ransomware

On November 9th, 2020, Bleeping Computer reported on a non-public advisory from Microsoft. The advisory indicates threat actors are using poisoned ad or search engine results to lure victims to sites masquerading as Microsoft Teams resulting in installation of malware. What follows is common human operated ransomware TTPs involving Cobalt Strike, privilege escalation, lateral movement and eventually deployment of ransomware. Based on publicly available information regarding this advisory, we are confident these incidents involving collaboration software are part of the same FakeUpdates campaign. Although we did not directly observe ransomware deployment resulting from these infections, information stealing malware is valuable as a precursor to ransomware deployment. The information collected from the system and network (including passwords) would be useful for initiating wider network compromise.

# Gaining The Foothold: Other Attack Vectors

While opportunistic malware has dominated eSentire's observations, gaining a foothold through exploitation of publicly facing applications and remote access services remain viable options for ransomware threats.

## Exploitation of Publicly Facing Applications

Unlike the constant barrage of spam mail, remote exploits have windows of effectiveness. These windows were numerous and wide over the last year. This was likely fueled by the ongoing corporate response to COVID-19, which spurred a transition to distributed remote corporate networks a.k.a the work-from-home era. During this time, organizations shifted to heavy usage of VPN, conference calling, and document collaboration tools. The reactive nature of deploying these systems prioritized business continuity over security considerations for the products as they were simultaneously coming into focus of threat actors. TRU has observed intruders attempting to deploy Netwalker ransomware after exploiting the SSL VPN, Pulse Secure and similar intrusion attempts stemming from a FortiGate exploit (the incident was intercepted before ransomware was observed).

### Top vulnerabilities exploited by ransomware threats:

- FiveHands - CVE-2021-20016 (SonicWall Secure Mobile Access SMA 100 series)
- Hello Kitty Ransomware - CVE-2019-0604 (Microsoft SharePoint)
- RansomEXX & Sodinokibi - CVE-2019-19781(Citrix ADC), CVE-2019-11510 (Pulse Secure PCS)
- RobinHood - CVE-2018-19320 (GIGABYTE APP Center v1.05.21 and earlier)
- Ryuk - CVE-2020-1472 (ZeroLogon)
- DearCry - CVE-2021-26855 (ProxyLogon, Microsoft Exchange)
- BlackKingdom - CVE-2021-26855 (ProxyLogon, Microsoft Exchange)
- Cring Ransomware - CVE-2018-13379 (FortiGate SSL VPN)

## Valid Credentials & External Remote Services

Another attack vector that arrives through remote access points is the use of valid credentials. Credentials obtained maliciously via phishing, past breaches or exploits can be used for entry into the network through VPN, RDP, or management software, depending on the type of credentials stolen. Email credentials, for example, can allow threat actors to abuse mail systems to distribute malware as a trusted sender, as observed in Spring 2020 during a REvil intrusion. In general, use of valid credentials can be a stealthy way to infiltrate a network, but multi-factor authentication and credential resets can mitigate against this initial access vector.



## Case Study: VPN Access Leads to Netwalker & Suncrypt Ransomware Attempt

**Date:** Fall 2020

**Who:** Education Organization

### Key Takeaways

This case demonstrates the capabilities of a persistent and motivated adversary in an attack involving a Ransomware-as-a-Service affiliate. When faced with detection and response actions, the adversary modified their attack with limited success. The eSentire SOC worked with the customer over the course of 24 hours to identify and remediate multiple attempts to access the customer's environment and deploy ransomware.

### What Happened

The customer's network was accessed through VPN using valid credentials for an employee. The adversary then used RDP to access critical servers and collect more credentials for the domain. The attack was identified, and the adversary's access was revoked from the network. The adversary returned later in the evening using different credentials and attempted to deploy both Suncrypt and Netwalker ransomware without success (the attempts to deploy the ransomware were blocked). They attempted to disable endpoint protection technology on the device but failed prior to being removed from the environment for a final time.

## Streamlining Opportunistic Attacks

Banking trojans are increasingly outfitted with reconnaissance commands that automatically profile a network and send the information to servers controlled by threat actors. These commands allow intrusion specialists to assess the value of the target and the effort required to deploy ransomware.

Trickbot was the first banking trojan to adopt this feature in 2018 alongside the developing ransomware intrusion model.

In 2020, TRU observed several other

banking trojans adopting this tactic, including IcedID, SocGhosh, and Qakbot. Throughout 2020, the same banking trojans were observed serving as the foothold in ransomware intrusion chains.

While some details and commands may vary, most take advantage of trusted windows processes, also known as LOLBINS (an acronym for "living-off-the-land binaries"). These commands are executed automatically upon landing on the system, then reported back through command-and-control. Similar to Trickbot, we assess these ransomware-linked banking trojans are leveraging this data to narrow down a wide list of network footholds into a small list of high-value targets. In May 2021, Qakbot was observed exhibiting this behavior at a financial services company, within an hour of reporting network information back through its C2 channel, Cobalt Strike and additional intrusion tools were dropped onto the machine prior to being contained by SOC analysts.

### Trickbot Reconnaissance

**ipconfig /all** – show all adapter TCP/IP configurations

**net config workstation** – shows what domain/workgroup the machine belongs to

**net view all** – display all available network shares

**nltest /domain\_trusts /all\_trusts** - list all trusted domains in the network

## Transitioning to Manual Intrusion Actions

Once a foothold has been gained via opportunistic attacks and value assessment have been made, the foothold can be utilized for manual intrusion actions. At this point, hands-on interaction is required to overcome the idiosyncrasies that occur in defense across organizations. For example, intruders have attempted to uninstall endpoint monitoring agents after failing to deploy ransomware, as seen in [eSentire's SunWalker Ransomware Battle Blog](#). eSentire has detected in-depth reconnaissance, credential theft, privilege escalation, and lateral movement at this phase. Threat actors leveraged offensive security tools like Cobalt Strike, PowerSploit, Bloodhound, Mimikatz, and Lazagne. Cobalt Strike and PowerSploit are intrusion framework suites that offer an array of tools that can be used selectively by an active intruder. Stopping the attack at this stage will require greater effort than earlier stages, as the attacker will be embedded in the environment.

## Actions-On-Objectives: Ransomware Deployment

After sufficient escalation is achieved, ransomware intruders can finally lockdown the network by deploying and executing ransomware payloads. Given the manual nature of this attack phase, ransomware deployment can occur in several unique ways, from manual drag and drop from an RDP session to manual command execution (PsExec) to abusing the legitimate technology (group policy, scheduled tasks, file shares, and remote management services).

### Deployment Techniques

- PsExec
- RDP session
- Group Policy from compromised DC
- File share and startup scripts
- Remote management product
- Cobalt Strike beacon session
- Scheduled tasks

## Ensuring the Payment: Extortion Tactics

Successful ransomware deployment results in leverage for the threat actors. This is the primary means through which threat actors extort payment from organizations. From 2019-2021, ransomware groups increasingly utilized a second form of extortion (aka "double extortion") in which sensitive data was downloaded and posted on leak sites – sometimes with a countdown timer. Around 63% of the RaaS offerings tracked by eSentire's TRU are known to have leak sites. If organizations fail to pay in a timely manner, not only is the ransom fee likely to increase, but threat actors will begin leaking sensitive information stolen during the intrusion. Additional tactics such as DDoS and contacting the organization's customers and affiliates have become common in 2021 (aka "triple" or "quadruple" extortion).

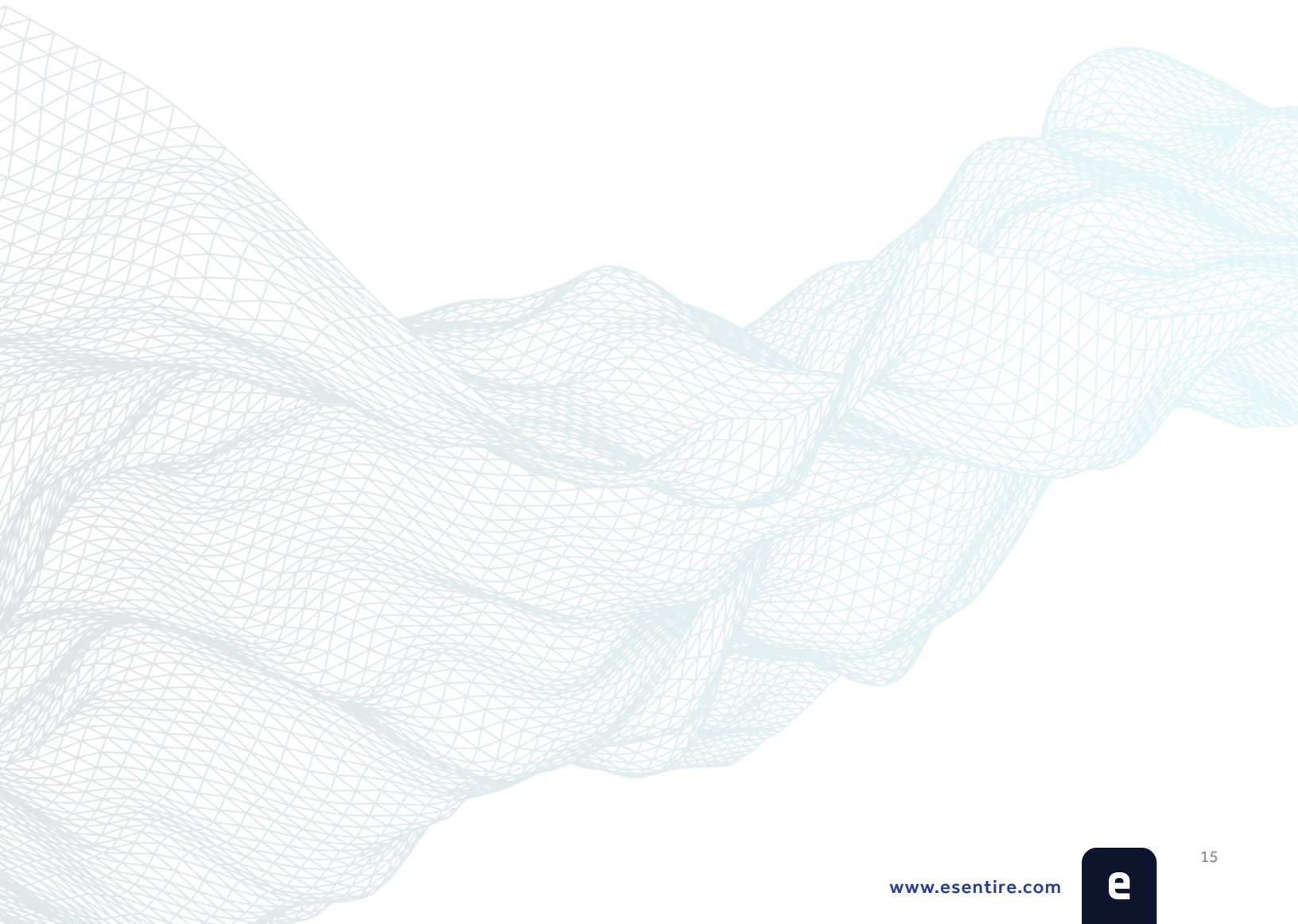
### Deployment Techniques

- DDoS during negotiations to increase pressure on victims (Avaddon, Darkside)
- Phone calls to Victim Organization (CLOP)
- Phone calls to affiliates/customers (CLOP)
- Network Connected Printers printing ransom notes (Egregor)
- Public Facebook Ads (Ragnar Locker)

# Conclusions

The emergence of new ransomware groups following the successful Ransomware-as-a-Service (RaaS) and double extortion models has made ransomware one of the most significant threats in recent years. Fully automated attacks are largely a thing of the past. Today's ransomware combines opportunistic attacks to cast a wide net from which high-value targets can be selected for further infiltration and ransomware deployment. Furthermore, commodity malware threats have adjusted their behavior to suit this target selection, suggesting money is to be made selling access to a network over committing bank fraud.

Prior to the current incarnation of ransomware, monetizing an intrusion required established infrastructure to sell information or launder stolen assets. Thanks to the RaaS model, anyone with access to a network and moderate intrusion skills has an opportunity to make money. While modern networks have arguably become better defended, the availability of offensive security tools such as Cobalt Strike has allowed less-skilled actors to punch above their weight and enter the fray. The result is a mix of established ransomware partnerships and unrelated ransomware affiliates working with RaaS offerings. This wide aperture for initial access and intrusion actions requires a holistic approach to defending environments, combining hardening measures and detection and response capabilities.



# How eSentire Can Help Combat Ransomware

Every malware case mentioned in this report arrived via social engineering methods, meaning the threat bypassed primary filtering mechanisms the organization had in place in their email systems or web browsers to successfully convince a user to execute malicious code. At eSentire, we assume that your preventative controls will be bypassed so we target known TTPs associated with each stage of ransomware attacks; from initial malware deployment to intrusion actions to ransomware. Successful identification at any stage results in immediate investigation and response actions by our 24/7 Security Operations Center Cyber Analysts and Elite Threat Hunters.

eSentire is recognized globally as the Authority in Managed Detection and Response because we hunt, investigate and stop known and unknown cyber threats before they disrupt your business. We were founded in 2001 to secure the environments of the world's most targeted industry - financial services. Over the last two decades we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale. With two 24/7 Security Operations Centers, hundreds of cyber experts, and 1000+ customers, across 70+ countries, we have demonstrated the ability to Own the R in MDR with a Mean Time to Contain of 15 minutes.

We deliver cyber program results through a combination of cutting-edge machine learning XDR technology, 24/7 threat hunting expertise and security operations leadership. eSentire offers comprehensive security services to support your business operations end-to-end as we stop breaches, simplify security and minimize your business risk:



## Managed Risk Services

Strategic services including Vulnerability Management, Managed Phishing and Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.



## Managed Detection and Response Services

We deliver complete and robust Response. By combining cutting-edge machine learning XDR, human security expertise and security operations leadership, we hunt and disrupt known & unknown threats before they impact your business.




## Digital Forensics and Incident Response Services

Battle-tested Incident Commander level expertise driving incident response, remediation, recovery, and root cause analysis. Emergency Preparedness and Emergency Response services as well as industry-leading 4-hour Threat Suppression SLA with eSentire IR Retainer available.

We have expertise in ransomware prevention, disruption and remediation. With a Mean Time to Contain threats of 15 minutes, and a 4-hour remote threat suppression SLA as part of our On Demand 24/7 Incident Response services, we provide critical time to value in driving your security outcomes forward.



<b>Ransomware Challenges</b>	<b>How We Help</b>
<b>24/7 Threat Detection</b>	<ul style="list-style-type: none"> <li>• 24/7 SOC Cyber Analysts monitor your environment and signals around the clock</li> <li>• Our team is armed with the latest investigation and response runbooks to identify and contain ransomware and precursor threats</li> <li>• eSentire MDR for Endpoint identifies and prevents ransomware-specific TTPs</li> </ul>
<b>Response to Intrusion</b>	<ul style="list-style-type: none"> <li>• Detection content for intrusion tools and associated techniques is deployed across eSentire MDR for Endpoint, Network and Managed Log services</li> <li>• We isolate, contain, respond and remediate ransomware threats</li> </ul>
<b>Email and Web Based Malware</b>	<ul style="list-style-type: none"> <li>• eSentire MDR for Endpoint identifies and prevents malware threats</li> <li>• eSentire MDR for Network identifies and disrupts malware network communication</li> <li>• eSentire Atlas XDR Cloud Platform disrupts known command and control (C2) channels across our global customer base automatically</li> </ul>
<b>Exploitation of Public Facing Assets</b>	<ul style="list-style-type: none"> <li>• eSentire Managed Vulnerability Service can identify and help you prioritize vulnerabilities exploited by ransomware threats</li> <li>• eSentire MDR for Network detects exploitation attempts at the network perimeter</li> </ul>
<b>Credential Replay Attacks Against Remote Access Services</b>	<ul style="list-style-type: none"> <li>• eSentire Managed Log identifies unusual authentication events and enables analysts to trace unauthorized network access</li> </ul>
<b>Emerging Threat Research</b>	<ul style="list-style-type: none"> <li>• eSentire's Threat Response Unit (TRU) actively monitors both internal and external threat data sources for actionable information</li> <li>• This knowledge is weaponized through new detection content, investigation runbooks, threat hunts and data analytics</li> </ul>

If you're experiencing a security incident or breach contact us  1-866-579-2200

# eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit [www.esentire.com](http://www.esentire.com) and follow @eSentire.