Infoblox

Q4 | 2021
CYBER THREAT REPORT

Powered by the
Infoblox Cyber Intelligence Group

Disclaimer

Infoblox publications and research are made available solely for general information purposes. The information contained in this publication is provided on an “as is” basis. Infoblox accepts no liability for the use of this data. Any additional developments or research since the date of publication will not be reflected in this report.

Table of Contents

Executive Summary

We at Infoblox are pleased to publish this edition of our Quarterly Cyber Threat Intelligence Report. We publish these reports during the first month of each calendar quarter.

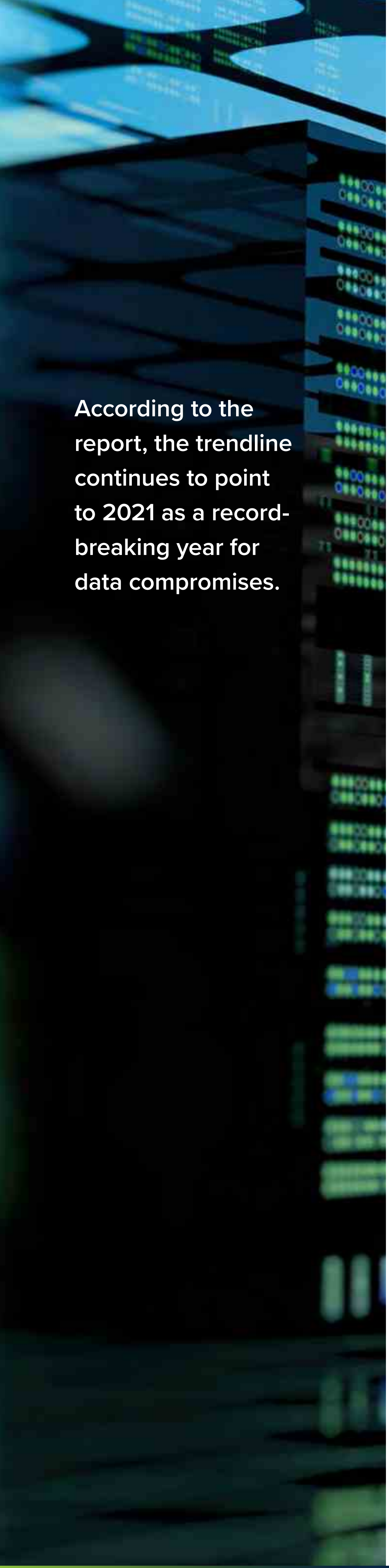
The Q4 2021 report includes our eight publicly released threat intelligence reports from October 1, 2021 to December 31, 2021. This quarter, we share third-party data for record-high numbers of data breaches in 2021 and for the emergence of phishing as the number-one attack vector behind those data breaches. We also share detailed information on DDoS Extortion and Mitigation, which is part of a comprehensive report produced by the Infoblox Threat Intelligence Group this quarter. Finally, we summarize important industry alerts, advisories and reports that the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the National Security Agency Central Security Service (NSA-CSS) published during this quarter.

This publication supplements our original research and insight into threats we observed leading up to and including this period of time. Our report includes a detailed analysis of advanced malware campaigns and of recent significant attacks. In some cases, we share and expand on original research published by other security firms, industry experts and university researchers. We feel that timely information on cyber threats is vital to protecting the community at large.

Usually, we report on specific threats and related data, customer impacts, analysis of campaign execution and attack chains, as well as vulnerabilities and mitigation steps. We also share background information on the attack groups likely responsible for the threats under review.

During Q4 2021, the Infoblox Threat Intelligence Group published the following reports on campaigns that delivered malware:

- Fake Delivery Spam Email Drops Ave Maria RAT - Published October 12, 2021
- Malspam Campaign Delivers Dark Crystal RAT (dcRAT) - Published October 12, 2021
- DDoS Extortion and Mitigation - Published October 18, 2021
- BlackMatter Ransomware - Published October 20, 2021
- SWIFT-Themed Malspam Delivers Vidar Infostealer - Published October 25, 2021
- New Malspam Campaign Delivers Adwind RAT - Published November 1, 2021
- New Threat Actor: PINK BOA - Published November 2, 2021
- Log4j Exploit Harvesting - Published December 13, 2021



According to the report, the trendline continues to point to 2021 as a record-breaking year for data compromises.

Data Breaches Heading to a New Record in 2021

According to the Identity Theft Resource Center's data breach analysis for Q3 of 2021, the total number of data compromises as of Q3 had already surpassed the total number of compromises in 2020. The report gave other disturbing statistics:

- The number of data breaches publicly reported at the end of Q3 (1,291) had exceeded the total number of data breaches in all of 2020 (1,108) by **17 percent**. The trendline continues to point to a record-breaking year for data compromises; the all-time high of 1,529 breaches was registered in 2017.
- The number of victims of data compromises increased dramatically in Q3, to a total of **~160 million individuals**, and most of it due to a series of data exposures that occurred in Q3.
- A trend is developing where organizations and state agencies do not include specifics about data compromises or do not report them soon.

Phishing Is the Leading Cause of Data Breaches in 2021

In its November 2021 Strategic Security Survey, Dark Reading (1) pointed out that phishing, malware, and denial-of-service attacks remained the most common causes of data breaches that organizations experienced in 2021 and (2) singled out phishing as the most common cause. According to the survey, the percentage of organizations reporting a phishing-related breach was slightly higher in 2021 (53 percent) than in 2020 (51 percent).

According to Dark Reading, *"concerns over attacks by state-sponsored threat actors are significantly higher than in the DarkReading survey last year and the year before. Sixteen percent of survey respondents expect that if they experience a data breach over the next year, a state sponsored threat actor would be the cause. That's almost double the 9 percent of respondents who said the same thing in our past two surveys."*

The survey also highlighted the following:

- **23 percent** of organizations that experienced data breaches reported network disruptions and unavailability of applications. 17 percent said they experienced a major financial loss, and 15 percent reported fraud.
- **16 percent** of the respondents described their organizations as more vulnerable to data breaches than in 2020. 56 percent said the vulnerability did not change.
- **48 percent** of the respondents said that if their organizations experience major data breaches in the next 12 months, the most likely cause would be human error.
- **33 percent** of organizations that experienced ransomware attacks ended up paying ransoms to get their data back.
- Fewer organizations are willing to disclose that they have fallen victim to ransomware attacks: 13 percent in 2020 and **only 4 percent** in 2021.
- **70 percent** of IT and security decision-makers believe that the attacks on Colonial Pipeline and JBS highlighted these and other organizations' inability to handle ransomware attacks effectively.

Anatomy of an Attack: DDoS Extortion and Mitigation

Overview

Distributed denial-of-service (DDoS) is a cyber attack that causes mass disruption of services. From 1996 (when first reports about DDoS attacks emerged) to 2010, threat actors used DDoS mainly to promote themselves or political agendas and to encourage social change; in recent years, the financial motive has been more prevalent and more DDoS activities have made extortion a major part of their strategy. In addition, prior to 2020, DDoS actors usually sent empty threats and did not follow up with attacks; since the second half of 2020, however, actors have made good on their threats and have followed up with attacks more frequently. Although threat actors have monetized DDoS threats and attacks in the past, we believe that popularization of cryptocurrency, willingness of some organizations to meet extortion demands (as was seen in the ransomware attack on Colonial Pipeline), and affordability of DDoS as a service (DDoSaaS) have encouraged threat actors to pursue these kinds of activities.

In nearly all recent attacks, the attackers have named themselves after well-known advanced persistent threat (APT) actors. Since 2014, companies across multiple industry verticals have received DDoS extortion letters from DDoS actors who have attempted to portray themselves as Cozy Bear, DDoS for Bitcoin (DD4BC), Sednit, Fancy Bear, Armada Collective, Lazarus, or Lazarus Group. The cyber intelligence community has not found a direct connection between the DDoS actors and the APT actors whose names they have borrowed. Usually, APT actors target specific kinds of entities according to a common characteristic, such as a geo-location or a business type; however, targets of the DDoS extortion campaigns are widely distributed across the globe and belong to various industries. Many researchers have speculated that the DDoS actors identify themselves as well-known APT actors to build credibility and increase the probability of extorting money from their targets.

The actors paused their campaigns for one month in spring 2020 but returned with new APT group names and enhanced tactics, techniques, and procedures (TTPs). Since then, the attacks have been more frequent and the extortion emails have come from dynamic addresses unique to the target organizations, not from static addresses that would include the actors' self-assumed aliases.

To perform a DDoS attack with enough power to disrupt enterprise-level services, threat actors use large botnets, which they can rent or develop. In addition, many actors use multiple attack vectors in one large assault; this makes mitigation difficult because no single DDoS protection system can resolve all types of attack methods. Over the past several years, actors who have successfully monetized DDoS campaigns via extortion have used the following DDoS attack vectors most often: DNS flood, DNS amplification, ARMS amplification, SNMP reflection, SYN flood, GRE flood, WS-discovery amplification, CLDAP reflection, TFTP amplification, NTP amplification, WordPress XML-RPC amplification, simple service discovery protocol (SSDP) and portmapper amplification.

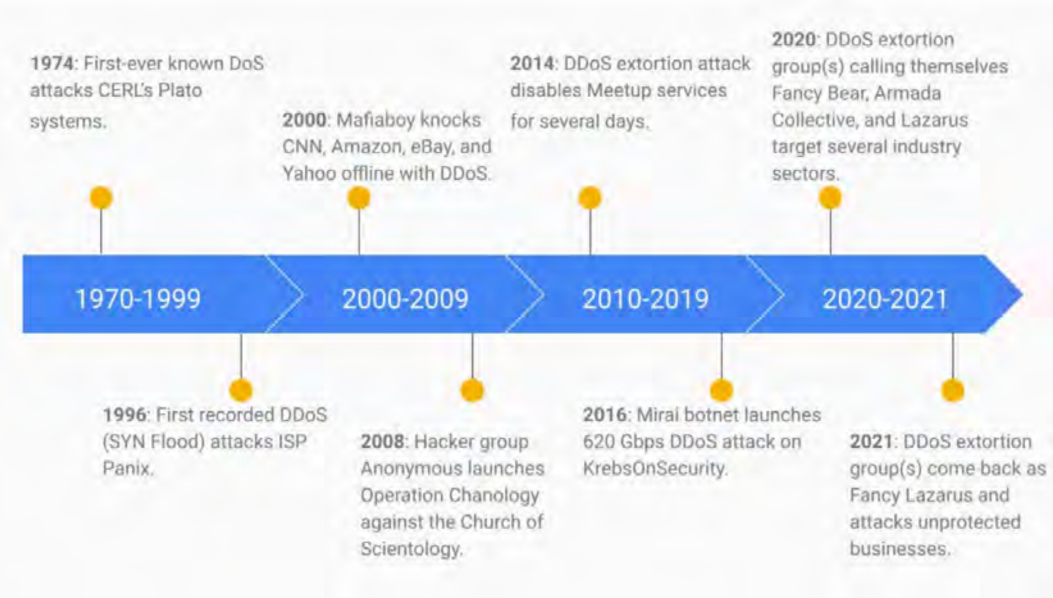
DDoS Timeline of News and Events

Since the first known occurrence of DDoS—the TCP SYN flood that took ISP Panix offline in 1996—threat actors have used DDoS to disable millions of legitimate services across various industries: energy, financial, insurance, manufacturing, public utilities, retail sectors, travel and hospitality, retail and e-commerce, high-tech and software, consumer packaged goods, and internet service providers. Up to 7.9 million DDoS attacks were reported in 2018 alone, and security researchers estimate that the number of attacks will reach 15 million some time in 2023. What compounds these numbers is that DDoS is one of the costliest cyber threats to mitigate, because it directly affects the availability of services crucial to business operations. Bulletproof's 2019 annual cybersecurity report indicated that a DoS or DDoS attack could cost a small company up to $120 thousand and a large company up to $2 million in damages.

In addition to TCP SYN flood, threat actors have used ICMP flood, UDP flood, and other basic DDoS attack instruments. However, as stress-testing and DDoS tools—such as Low Orbit Ion Cannon (LOIC) and High Orbit Ion Cannon (HOIC)—become more affordable, the attacks become more complex and numerous. Also, more DDoS campaigns have used a combination of multiple attack vectors in a single attack. These factors make it increasingly difficult for providers of network services to protect their infrastructure, because no single security solution can protect against all DDoS attack vectors. Furthermore, new DDoS attack vectors have emerged—Constrained Application Protocol (CoAP), Web Services Dynamic Discovery (WS-DD), Apple Remote Management Service (ARMS), and Jenkins web-based automation software—and cyber criminals have used all of them to launch DDoS attacks.

The following timeline describes the most notable events in the history of DDoS and discusses newly discovered attack vectors and actors, campaigns that have had high impact on business, and development of game-changing mitigation solutions. The timeline suggests that the objectives of DDoS attacks have shifted from personal notoriety and vandalism to achieving lucrative gains by following mature business models.

Figure 1: Timeline of DDoS Attacks



1974: First-ever known DoS attacks CERL's Plato systems.

1996: First recorded DDoS (SYN Flood) attacks ISP Panix.

2000: Mafiaboy knocks CNN, Amazon, eBay, and Yahoo offline with DDoS.

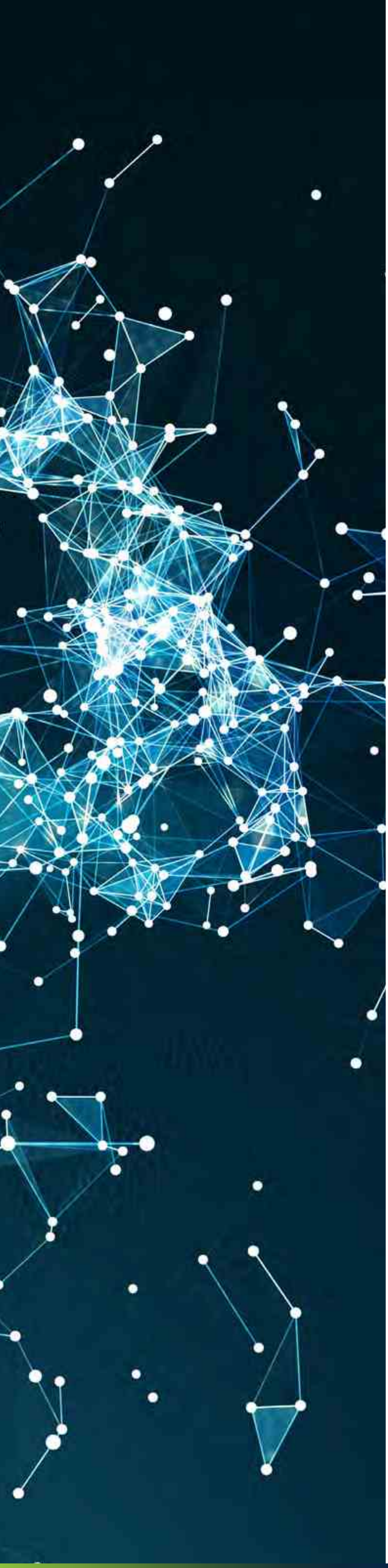
2008: Hacker group Anonymous launches Operation Chanology against the Church of Scientology.

2014: DDoS extortion attack disables Meetup services for several days.

2016: Mirai botnet launches 620 Gbps DDoS attack on KrebsOnSecurity.

2020: DDoS extortion group(s) calling themselves Fancy Bear, Armada Collective, and Lazarus target several industry sectors.

2021: DDoS extortion group(s) come back as Fancy Lazarus and attacks unprotected businesses.



Categories of DDoS Attacks

At a high level, DDoS attacks can be categorized as volumetric, application-layer, or protocol-based. They typically target layers 3, 4 and 7 in the Open Systems Interconnection (OSI) model.

- Volumetric DDoS attacks exploit mostly layer 7 protocols, especially the DNS and network time protocol (NTP), and they attempt to reduce a network's bandwidth capacity by flooding the network with heavy traffic or with request packets. Some volumetric DDoS attacks are large enough to max out the bandwidth capacity of upstream internet service providers or data centers, and this prevents legitimate traffic from connecting to websites.

  Because generating a high number of requests is relatively easy, volumetric attacks are popular among DDoS actors. The requests are small, but they command a large response to a victim's server, such as a DNS resolver.

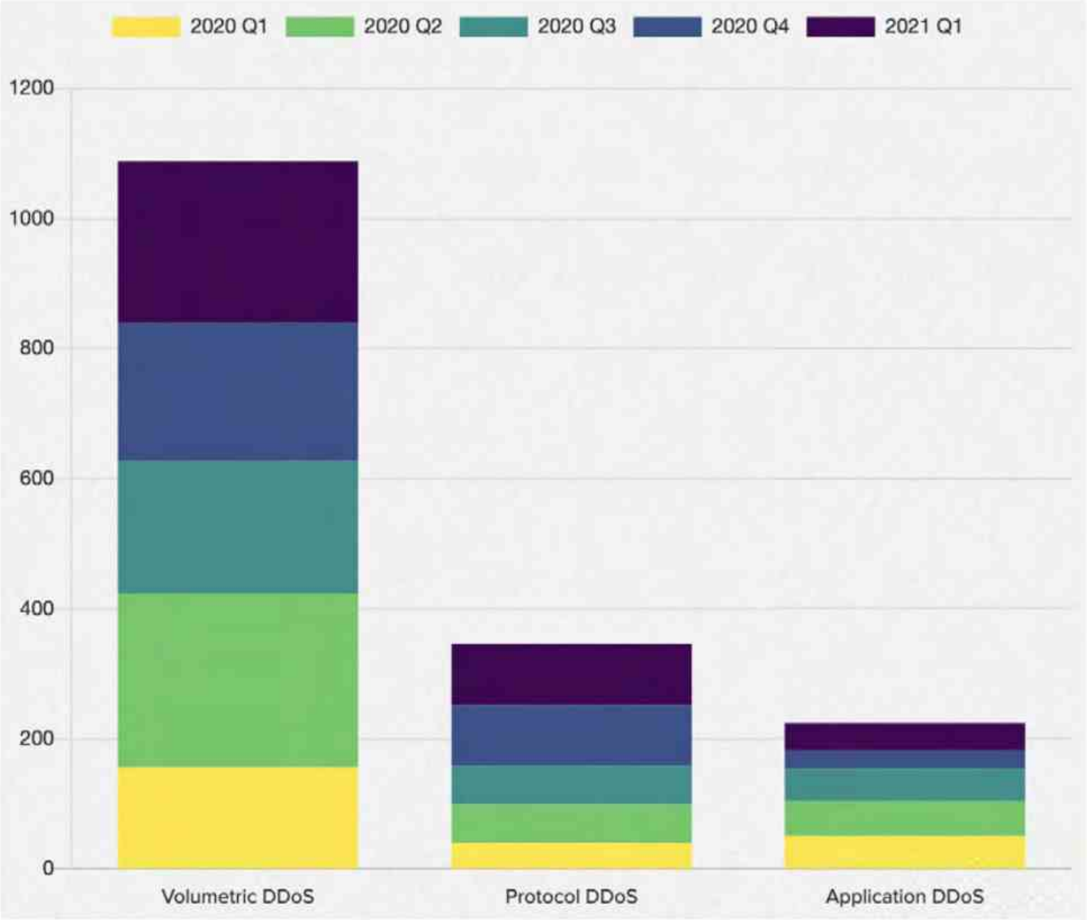
- Like volumetric attacks, application-layer DDoS attacks target mostly layer 7 protocols. Unlike volumetric attacks, they try to exhaust server resources by attacking applications' backend processes that are computationally expensive. In addition, they generate less traffic and use less total bandwidth but can inflict at least as much damage. To direct their requests, the attackers who operate an application-layer attack must have deep knowledge of the application and its supporting endpoints.

  Application-layer attacks are effective because the server expends considerably more resources in responding to requests than the client does in generating them. If the conditions are right—for example, if the target application is not optimized or cannot manage CPU- and RAM-intensive operations because of limited resources—some attacks can disable web applications by using just one machine.

- Protocol-based DDoS attacks target weaknesses in protocols in layers 3 and 4. These kinds of attacks are difficult to mitigate, because the majority of online devices use internet communication protocols. Even if vendors release security patches relatively quickly, businesses might take a long time to deploy them, because the patches are often incompatible with existing systems.

  One of the oldest (first detected in 2014) and most common types of protocol-based DDoS attacks is a TCP synchronization (SYN) flood. To a victim's server, a DDoS actor sends a large number of SYN packets that contain a modified source address, which hides the sender's identity. The victim's server responds to each connection request and leaves a port open to receiving the final ACK packet. However, the actors do not send the ACK packet but continue to send additional SYN packets until the server exhausts all available ports. This prevents the server from processing legitimate requests and running other operations.

Figure 2: DDoS attacks by type, from January 2020 to March 2021



Attack Chains

DDoS extortion campaigns typically follow one of two kinds of attack chains:

- The actors start with a DDoS demonstration: a show of force and an attempt to convince the attacked organization that the threat is real. The actors target a specific resource that belongs to the attacked organization's web service or network infrastructure. The demonstration is large enough to slow down the organization's services but not large enough to knock them offline.

  After or during the demonstration, the actors send an extortion email, where they threaten to launch a larger DDoS attack if the organization does not make a specified bitcoin payment to the actors' cryptocurrency wallet. If the organization does not make the payment by the deadline, the actors follow up with the main DDoS attack and increase the extortion amount every day after the due date, until they receive the full payment.

- The actors send the extortion email before the attack. The email contains the extortion demand, bitcoin wallet address, deadline, the attack's capacity, and other details. The group might also use the email to boast about their ability to send several terabytes' worth of traffic packets per second. In most cases, these threats are not bluffs and are followed by full-scale attacks.

Mitigation

When planning for DDoS mitigation, organizations should consider not only their business obligation to keep services running but also the amount of service disruption they and their customers can tolerate. The Australian Cyber Security Centre provides some basic guidance that organizations can take to reduce the likelihood and potential impact of a DDoS attack:

- Determine which functionality is truly critical to the operations of an organization. Create all backups necessary to keep it running despite the attack, and allocate enough resources (if necessary, by moving them from non-critical functionality) to maintain it during the attack and, ultimately, to restore it once the attack has been managed.
- With service providers, discuss the details of DDoS prevention and mitigation strategies, namely:
    - The capacity to withstand DDoS attacks
    - Any costs likely to be incurred by customers
    - Thresholds for notifying customers or for turning off their online services during DDoS attacks
    - Pre-approved actions that can be taken during DDoS attacks
    - Arrangements made with upstream (for example, Tier 2) service providers to block malicious traffic as far upstream as possible
- Protect an organization's domain names by using registrar locking and by confirming that the domain registration details are correct.
- Ensure that customers maintain details of their service providers' 24x7 contacts and that service providers maintain details of their customers' 24x7 contacts.
- Establish additional out-of-band contact details—for example, mobile phone numbers and non-organizational email addresses—that service providers would use if normal communication channels were to fail.
- To detect DDoS attacks and measure their impact, implement availability monitoring with real-time alerting.
- Prepare a static version of the company's website. Ensure that it not only facilitates continuity of service during a DDoS attack but also requires minimal processing and bandwidth.
- Use cloud-based hosting from a major cloud service provider—preferably from several major cloud service providers, to ensure redundancy—with high-bandwidth content delivery networks that cache non-dynamic websites. If using a content-delivery network, avoid disclosing the IP address of the web server that is under the organization's control (referred to as the origin web server), and use a firewall to ensure that only the content-delivery network can access this web server.

- Use a DDoS mitigation service because it offers a variety of in-depth defense approaches that can be implemented in the infrastructure and application layers.

An effective DDoS mitigation posture will take into account all requirements and constraints of a business, and it will implement controls focused on cloud infrastructure, on-premise systems, or a hybrid of thereof. As a general rule, the more complex the mitigation system, the more likely it is to fail due to misconfigurations or failed integration points. Organizations that are considering DDoS protection for the first time should start with simple systems that can be monitored and refined. As are other types of cyber attacks, DDoS attacks are constantly evolving in complexity and effectiveness; for this reason, cyber defenders must never stop improving their TTPs and defenses. This approach applies to DDoS mitigations, which require careful planning to ensure adequate maintenance and cutting-edge protection.

Read the rest of this special 35-page report by the Infoblox Threat Intelligence Group here.

Cybersecurity & Infrastructure Security Agency (CISA) Alerts in Q4 2021

AA21-356A: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ), the New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) are releasing this joint Cybersecurity Advisory (CSA) to provide mitigation guidance on addressing vulnerabilities in Apache's Log4j software library: CVE-2021-44228 (known as "Log4Shell"), CVE-2021-45046 and CVE-2021-45105. Sophisticated cyber threat actors are actively scanning networks to potentially exploit Log4Shell, CVE-2021-45046, and CVE-2021-45105 in vulnerable systems. According to public reporting, Log4Shell and CVE-2021-45046 are being actively exploited.

CISA, in collaboration with industry members of CISA's Joint Cyber Defense Collaborative (JCDC), previously published guidance on Log4Shell for vendors and affected organizations in which CISA recommended that affected organizations immediately apply appropriate patches (or apply workarounds if unable to upgrade), conduct a security review, and report compromises to CISA or the FBI. CISA also issued an Emergency Directive directing U.S. federal civilian executive branch (FCEB) agencies to immediately mitigate Log4j vulnerabilities in solution stacks that accept data from the internet. This joint CSA expands on the previously published guidance by detailing steps that vendors and organizations with IT and/or cloud assets should take to reduce the risk posed by these vulnerabilities.

Click here for a PDF version of this report.

AA21-336A: APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to highlight the cyber threat associated with active exploitation of a newly identified vulnerability (CVE-2021-44077) in Zoho ManageEngine ServiceDesk Plus—IT help desk software with asset management.

CVE-2021-44077, which Zoho rated critical, is an unauthenticated remote code execution (RCE) vulnerability affecting all ServiceDesk Plus versions up to, and including, version 11305. This vulnerability was addressed by the update released by Zoho on September 16, 2021, for ServiceDesk Plus versions 11306 and above. The FBI and CISA assess that advanced persistent threat (APT) actors are among those exploiting the vulnerability. Successful exploitation of the vulnerability allows an attacker to upload executable files and place webshells, which enable the

adversary to conduct post-exploitation activities, such as compromising administrator credentials, conducting lateral movement and exfiltrating registry hives and Active Directory files.

The Zoho update that patched this vulnerability was released on September 16, 2021 along with a security advisory. Additionally, an email advisory was sent to all ServiceDesk Plus customers with additional information. Zoho released a subsequent security advisory on November 22, 2021 and advised customers to patch immediately.

Click here for a PDF version of this report.

Click here for indicators of compromise (IOCs) in STIX format.

AA21-321A: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities

This joint cybersecurity advisory is the result of an analytic effort among the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC) and the United Kingdom's National Cyber Security Centre (NCSC) to highlight ongoing malicious cyber activity by an advanced persistent threat (APT) group that FBI, CISA, ACSC and NCSC assess is associated with the government of Iran. FBI and CISA have observed this Iranian government-sponsored APT group exploiting Fortinet vulnerabilities since at least March 2021 and a Microsoft Exchange ProxyShell vulnerability since at least October 2021 to gain initial access to systems in advance of follow-on operations, which include deploying ransomware. ACSC is also aware that this APT group has used the same Microsoft Exchange vulnerability in Australia.

The Iranian government-sponsored APT actors are actively targeting a broad range of victims across multiple U.S. critical infrastructure sectors, including the Transportation Sector and the Healthcare and Public Health Sector, as well as Australian organizations. FBI, CISA, ACSC and NCSC assess the actors are focused on exploiting known vulnerabilities rather than targeting specific sectors. These Iranian government-sponsored APT actors can leverage this access for follow-on operations, such as data exfiltration or encryption, ransomware and extortion.

This advisory provides observed tactics and techniques, as well as indicators of compromise (IOCs) that FBI, CISA, ACSC and NCSC assess are likely associated with this Iranian government-sponsored APT activity.

The FBI, CISA, ACSC and NCSC urge critical infrastructure organizations to apply the recommendations listed in the Mitigations section of this advisory to mitigate risk of compromise from Iranian government-sponsored cyber actors.

For a downloadable copy of IOCs, see AA21-321A.stix.

For more information on Iranian government-sponsored malicious cyber activity, see us-cert.cisa.gov/Iran.

Click here for a PDF version of this report.

AA21-291A: BlackMatter Ransomware

This joint Cybersecurity Advisory was developed by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) to provide information on BlackMatter ransomware. Since July 2021, BlackMatter ransomware has targeted multiple U.S. critical infrastructure entities, including two U.S. Food and Agriculture Sector organizations.

This advisory provides information on cyber actor tactics, techniques and procedures (TTPs) obtained from a sample of BlackMatter ransomware analyzed in a sandbox environment as well as from trusted third-party reporting. Using embedded, previously compromised credentials, BlackMatter leverages the Lightweight Directory Access Protocol (LDAP) and Server Message Block (SMB) protocol to access the Active Directory (AD) to discover all hosts on the network. BlackMatter then remotely encrypts the hosts and shared drives as they are found.

Ransomware attacks against critical infrastructure entities could directly affect consumer access to critical infrastructure services; therefore, CISA, the FBI and NSA urge all organizations, including critical infrastructure organizations, to implement the recommendations listed in the Mitigations section of this joint advisory. These mitigations will help organizations reduce the risk of compromise from BlackMatter ransomware attacks.

Click here for a PDF version of this report.

AA21-287A: Ongoing Cyber Threats to U.S. Water and Wastewater Systems

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA) and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities. This activity—which includes attempts to compromise system integrity via unauthorized access—threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities.

To secure WWS facilities—including Department of Defense (DoD) water treatment facilities in the United States and abroad—against the TTPs listed below, CISA, FBI, EPA and NSA strongly urge organizations to implement the measures described in the Recommended Mitigations section of this advisory.

Click here for a PDF version of this report.

Federal Bureau of Investigation (FBI) IC3 Industry Alerts in Q4 2021

APT Actors Exploiting Newly-Identified Zero Day in ManageEngine Desktop Central – December 20, 2021

Since at least late October 2021, APT actors have been actively exploiting a zero-day, now identified as CVE-2021-44515, on ManageEngine Desktop Central servers. The APT actors were observed compromising Desktop Central servers, dropping a webshell that overrides a legitimate function of Desktop Central, downloading post-exploitation tools, enumerating domain users and groups, conducting network reconnaissance, attempting lateral movement and dumping credentials. CVE-2021-44515, which Zoho rated critical, addresses an authentication bypass vulnerability in ManageEngine Desktop Central software that can allow an adversary to bypass authentication and execute arbitrary code on Desktop Central servers.

Indicators of Compromise Associated with Cuba Ransomware (Revised) – December 3, 2021

The FBI has identified, as of early November 2021 that Cuba ransomware actors have compromised at least 49 entities in five critical infrastructure sectors, including but not limited to the financial, government, healthcare, manufacturing, and information technology sectors. Cuba ransomware is distributed through Hancitor malware, a loader known for dropping or executing stealers, such as Remote Access Trojans (RATs) and other types of ransomware, onto victims' networks. Hancitor malware actors use phishing emails, Microsoft Exchange vulnerabilities, compromised credentials, or legitimate Remote Desktop Protocol (RDP) tools to gain initial access to a victim's network. Subsequently, Cuba ransomware actors use legitimate Windows services—such as PowerShell, PsExec, and other unspecified services—and then leverage Windows Admin privileges to execute their ransomware and other processes remotely. Cuba ransomware actors compromise a victim network through the encryption of target files with the ".cuba" extension. Cuba ransomware actors have demanded at least US $74 million and received at least US $43.9 million in ransom payments.

APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus – December 3, 2021

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to highlight the cyber threat associated with active exploitation of a newly identified vulnerability (CVE-2021-44077) in Zoho ManageEngine ServiceDesk Plus—IT help desk software with asset management. CVE-2021-44077, which Zoho rated critical, is an unauthenticated remote code execution (RCE) vulnerability affecting all ServiceDesk Plus versions up to, and including, version 11305. This vulnerability was

addressed by the update released by Zoho on September 16, 2021, for ServiceDesk Plus versions 11306 and above. The FBI and CISA assess that advanced persistent threat (APT) actors are among those exploiting the vulnerability. Successful exploitation of the vulnerability allows an attacker to upload executable files and place webshells, which enable the adversary to conduct post-exploitation activities, such as compromising administrator credentials, conducting lateral movement and exfiltrating registry hives and Active Directory files.

An APT Group Exploiting a 0-day in FatPipe WARP, MPVPN and IPVPN Software – November 17, 2021

As of November 2021, FBI forensic analysis indicated exploitation of a 0-day vulnerability in the FatPipe MPVPN® device software1 going back to at least May 2021. The vulnerability allowed APT actors to gain access to an unrestricted file upload function to drop a webshell for exploitation activity with root access, leading to elevated privileges and potential follow-on activity. Exploitation of this vulnerability then served as a jumping off point into other infrastructure for the APT actors. This vulnerability is not yet identified with a CVE number but can be located with the FatPipe Security Advisory number FPSA006. The vulnerability affects all FatPipe WARP®, MPVPN and IPVPN® device software prior to the latest version releases 10.1.2r60p93 and 10.2.2r44p1.

Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities – November 17, 2021

As of November 2021, FBI forensic analysis indicated exploitation of a 0-day vulnerability in the FatPipe MPVPN® device software1 going back to at least May 2021. The vulnerability allowed APT actors to gain access to an unrestricted file upload function to drop a webshell for exploitation activity with root access, leading to elevated privileges and potential follow-on activity. Exploitation of this vulnerability then served as a jumping off point into other infrastructure for the APT actors. This vulnerability is not yet identified with a CVE number but can be located with the FatPipe Security Advisory number FPSA006. The vulnerability affects all FatPipe WARP®, MPVPN and IPVPN® device software prior to the latest version releases 10.1.2r60p93 and 10.2.2r44p1.

Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims – November 1, 2021

Ransomware actors are targeting companies involved in significant, time-sensitive financial events to incentivize ransom payment by these victims. Ransomware is often a two-stage process beginning with an initial intrusion through a trojan malware, which allows an access broker to perform reconnaissance and determine how to best monetize the access. However, while this malware is often mass distributed, most victims of trojans are not also victims of ransomware, indicating ransomware targets are often carefully selected from a pool based on information gleaned from the initial reconnaissance. During the initial reconnaissance phase, cyber criminals identify non-publicly available information, which they threaten to release or use as leverage during the extortion to entice victims to comply with ransom demands. Impending events that could affect a victim's stock value, such as announcements, mergers and acquisitions, encourage ransomware actors to target a network or adjust their timeline for extortion where access is established.

Tactics, Techniques and Indicators of Compromise Associated with Hello Kitty/FiveHands Ransomware – October 29, 2021

The FBI first observed Hello Kitty/FiveHands ransomware in January 2021. Hello Kitty/FiveHands actors aggressively apply pressure to victims typically using the double extortion technique. In some cases, if the victim does not respond quickly or does not pay the ransom, the threat actors will launch a distributed denial-of-service (DDoS) attack on the victim company's public facing website. Hello Kitty/FiveHands actors demand varying ransom payments in Bitcoin (BTC) that appear tailored to each victim, commensurate with their assessed ability to pay it. If no ransom is paid, the threat actors will post victim data to the Babuk site (payload.bin) or sell it to a third-party data broker.

Indicators of Compromise Associated with Ranzy Locker Ransomware – October 26, 2021

The FBI first identified Ranzy Locker ransomware in late 2020 when the variant began to target victims in the United States. Unknown cyber criminals using Ranzy Locker ransomware had compromised more than 30 US businesses as of July 2021. The victims include the construction subsector of the critical manufacturing sector, the academia sub sector of the government facilities sector, the information technology sector and the transportation sector.

A majority of victims reported the actors conducted a brute force attack targeting Remote Desktop Protocol (RDP) credentials to gain access to the victims' networks. Recent victims reported the actors leveraged known Microsoft Exchange Server vulnerabilities and phishing as the means of compromising their networks. The actors attempted to locate important files to exfiltrate, such as customer information, PII related files and financial records. Ranzy Locker is deployed to encrypt files on compromised Windows host systems (including servers and virtual machines) and attached network shares. The Ranzy Locker executable leaves a ransom note in all directories where encryption occurred demanding the victim pay a ransom in exchange for a decryption tool. In an example of double extortion techniques, Ranzy actors in some cases have demanded a second ransom from the victim in exchange for not leaking the data on the internet.

BlackMatter Ransomware – October 19, 2021

This joint Cybersecurity Advisory was developed by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) to provide information on BlackMatter ransomware. Since July 2021, BlackMatter ransomware has targeted multiple

U.S. critical infrastructure entities, including two U.S. Food and Agriculture Sector organizations. This advisory provides information on cyber actor tactics, techniques and procedures (TTPs) obtained from a sample of BlackMatter ransomware analyzed in a sandbox environment as well as from trusted third-party reporting. Using embedded, previously compromised credentials, BlackMatter leverages the Lightweight Directory Access Protocol (LDAP) and Server Message Block (SMB) protocol to access the Active Directory (AD) to discover all hosts on the network. BlackMatter then remotely encrypts the hosts and shared drives as they are found.

Ongoing Cyber Threats to U.S. Water and Wastewater Systems – October 14, 2021

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA) and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems, and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities. This activity—which includes attempts to compromise system integrity via unauthorized access—threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities. Note: although cyber threats across critical infrastructure sectors are increasing, this advisory does not intend to indicate specific targeting of the WWS Sector versus others. To secure WWS facilities—including Department of Defense (DoD) water treatment facilities in the United States and abroad—against the TTPs listed below, CISA, FBI, EPA and NSA strongly urge organizations to implement the measures described in the Recommended Mitigations section of this advisory.

National Security Agency/ Central Security Service (NSA-CSS) Advisories and Guidance in Q4 2021

Mitigating Log4Shell and Other Log4j-Related Vulnerabilities

Summary

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ), the New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) are releasing this joint Cybersecurity Advisory (CSA) to provide mitigation guidance on addressing vulnerabilities in Apache's Log4j software library: CVE-2021-44228 (known as "Log4Shell"), CVE-2021-45046 and CVE-2021-45105. Sophisticated cyber threat actors are actively scanning networks to potentially exploit Log4Shell, CVE-2021-45046, and CVE-2021-45105 in vulnerable systems. According to public reporting, Log4Shell and CVE-2021-45046 are being actively exploited.

Click here for the complete PDF version of this advisory.

Security Guidance for 5G Cloud Infrastructures – Part III: Data Protection

A 5G Cloud Infrastructure comprises four security domains:

1. **Workload:** Virtual network functions (VNF) and cloud native network functions (CNF, previously referred to as Containerized Network Functions) deployed on virtual machines or containers, respectively.
2. **Platform:** Hardware, software and network that supports workloads.
3. **Front-end Networks:** Network connectivity between the platform and other networks.
4. **Back-end Networks:** Network connectivity between the platform and Data Center Operations.

Part III focuses on protecting the confidentiality and integrity of data within a 5G cloud infrastructure. Data confidentiality measures should be designed to protect sensitive information from unauthorized access. Data integrity ensures that data is not tampered with or altered by unauthorized access. Authenticity mechanisms play a key role in data protection by confirming users and systems are authorized with the correct rights to access the 5G cloud infrastructure data.

Click here for the complete PDF version of this advisory.

Security Guidance for 5G Cloud Infrastructures – Part II: Securely Isolate Network Resources

Pods are the isolated environments used to execute 5G network functions in a 5G container centric or hybrid container/virtual network function design and deployment. Pods provide highly configurable, flexible workloads that can be scaled and orchestrated from a central control plane, while enforcing isolation of each workload. The scale and interoperability requirements of 5G cloud components makes securely configuring Pods a challenging but important ongoing effort. A strong Pod security posture leverages containerization technology to harden the deployed application, protects interactions between Pods and detects malicious/anomalous activity within the cluster.

Part II of this four-part series will describe several aspects of Pod security including:

- Strengthening Pod isolation, such as limiting permissions on deployed containers
- Cryptographically isolating critical Pods using trusted execution environments
- Using best practices to avoid resource contention & DOS attacks
- Implementing container image security through build processes, scanning and enhancements to the trust environment
- Implementing real-time threat detection through minimizing noise, curating baseline behavior and alerting on anomalous activity.

Click here for the complete PDF version of this advisory.

Security Guidance for 5G Cloud Infrastructures – Part I: Prevent and Detect Lateral Movement

Part I of this series presents guidance for mitigating lateral movement attempts by attackers who have successfully exploited a vulnerability to gain initial access into a 5G cloud system. Although this part focuses on a few critical areas, from a Zero Trust perspective, following the guidance provided in the other three parts of this series is equally important.

Implement Secure Identity and Access Management (IDAM) in the 5G Cloud

After the initial compromise of a network, attackers commonly pivot laterally by exploiting the availability of internal services, particularly looking for services that are unauthenticated. For example, an attacker might use an initial position on a compromised virtual machine (VM) or container to access an application programming interface (API) or service endpoint that is not exposed externally. 5G cloud deployments will introduce more opportunities to move laterally in this manner because they support new implementations such as Service-Based Architecture (SBA), containers and VMs that result in more element-to-element communications than in previous networks that utilized physical appliances and point-to-point interfaces. Reducing the risk of these types of attacks, both at the network-function layer as well as the underlying cloud infrastructure layer, is a critical activity for reducing the overall risk of lateral movement. Audience: Cloud Providers, Mobile Network Operators

Guidance/Mitigations

- 5G networks should assign unique identities to all elements (and preferably to each interface) that will communicate to other elements in the 5G network.
- Before allowing access to a resource (e.g. Application Programming Interface [API], Command Line Interface [CLI]), each network element should authenticate and authorize the entity requesting access.
- Where possible, identities should be assigned using Public Key Infrastructure X.509 certificates from a trusted certificate authority (CA) rather than username/password combinations.
- If username/passwords must be used, multi-factor authentication (MFA) should be enabled to reduce the risk of compromise.
- The 5G network should provide automated mechanisms for credential management, especially as these features become more readily integrated in modern cloud environments (e.g., certificate rotation via a Service Mesh).
- Where possible, use certificate pinning or public key pinning to provide additional identity assurance when authentication is dependent upon multiple CAs. Certificate pinning and public key pinning associate a host with an expected certificate reducing the impact from a compromised CA.
- All access to resources should be logged. Each log entry should contain the time, resource, requesting entity (name or service), information about the requesting entity's location (region, IP address) and result of the access request (allow, deny). Logs should be protected as described in Part III: Protect Data in Transit, In-Use and at Rest of this series.
- Analytics for detecting potentially malicious resource access attempts should be deployed and run regularly.

Click here for the complete PDF version of this advisory.

Ongoing Cyber Threats to the U.S. Water and Wastewater Systems

Joint Cybersecurity Advisory published by CISA, the FBI and the NSA

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA) and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities. This activity—which includes attempts to compromise system integrity via unauthorized access—threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities. Note: although cyber threats across critical infrastructure sectors are increasing, this advisory does not intend to indicate specific targeting of the WWS Sector versus others.

To secure WWS facilities—including Department of Defense (DoD) water treatment facilities in the United States and abroad—against the TTPs listed below, CISA, FBI, EPA and NSA strongly urge organizations to implement the measures described in the Recommended Mitigations section of this advisory.

Click here for the complete PDF version of this advisory.

Avoid Dangers of Wildcard TLS Certificates and the ALPACA Technique

National Security Agency | Cyber Security Information Sheet

Wildcard certificates are often used to authenticate multiple servers, saving organizations time and money. Wildcard certificates have legitimate uses, but can confer risk from poorly secured servers to other servers in the same certificate's scope.

A new style of web application exploitation, dubbed "ALPACA," increases the risk from using broadly scoped wildcard certificates to verify server identities during the Transport Layer Security (TLS) handshake. Application Layer Protocols Allowing Cross-Protocol Attack (ALPACA) is a technique used to exploit hardened web applications through non-HTTP (Hypertext Transfer Protocol) services secured using the same or a similar TLS certificate. This Cyber Security Information Sheet details the risks from wildcard certificates and ALPACA, and provides mitigations for both.

Administrators should assess their environments to ensure that their certificate usage, especially the use of wildcard certificates, does not create unmitigated risks, and in particular, that their organizations' web servers are not vulnerable to ALPACA techniques.

Click here for the complete PDF version of this advisory.

Infoblox Threat Reports and Cyber Threat Alerts in Q4 2021

Fake Delivery Spam Email Drops Ave Maria RAT – October 12, 2021

On October 5 and 6, Infoblox observed that a malspam campaign was distributing the remote access trojan (RAT) Ave Maria through a Microsoft Word file. The threat actors were using a DHL-themed lure to entice the targets into opening the malicious attachment. Ave Maria was first seen at the end of 2018, and cybersecurity company Yoroi first reported on it at the beginning of 2019. We have reported on Ave Maria campaigns in 2019 and 2020.

Read the entire Cyber Campaign Brief here.

Malspam Campaign Delivers Dark Crystal RAT (dcRAT) – October 12, 2021

From September 30 to October 4, Infoblox observed a malicious email campaign distributing dcRAT. This malware is propagated via a Microsoft Word document that contains a malicious VBA script.

A May 2020 report said that dcRAT was being sold on hxxp://dcrat[.]ru. Since then, the site has been taken down, the content of the landing page has been replaced with Russian profanities, and distribution of dcRAT has shifted to hacking forums and P2P platforms.

Read the entire Cyber Campaign Brief here.

DDoS Extortion and Mitigation – October 18, 2021

Distributed denial-of-service (DDoS) is a cyber attack that causes mass-disruption of services. From 1996 (when first reports about DDoS attacks emerged) to 2010, threat actors primarily used DDoS for promoting themselves or political agendas and for encouraging social change; in recent years, the financial motive has been more prevalent, and more DDoS activities have made extortion a major part of their strategy. In addition, prior to 2020, DDoS actors usually sent empty threats and did not follow up with attacks; since the second half of 2020, and throughout 2021, actors have made good on their threats and have followed up with attacks more frequently. Although threat actors have monetized DDoS threats or attacks in the past, we believe that the popularization of cryptocurrency, willingness of some organizations to meet extortion demands (as was seen in the ransomware attack on Colonial Pipeline), and the affordability of DDoS-as-a-service (DDoSaaS) have encouraged threat actors to pursue these kinds of activities.

Read the entire Cyber Campaign Brief here.

SWIFT-Themed Malspam Delivers Vidar Infostealer – October 25, 2021

On October 20, Infoblox observed a malicious email campaign distributing the infostealer Vidar and using a SWIFT payment theme in the messages. The features of the Vidar file used in this campaign closely resembled those of the Vidar file we observed last year.

Vidar was first discovered in October 2018. It is written in C++ and is a variant of the Arkei infostealer. The developers of Vidar sell it as a malware as a service (MaaS), and cyber criminals can customize and control it through a web control panel.

After compromising a victim's machine, Vidar exfiltrates data from web browsers, cryptocurrency wallets, messenger software, and two-factor authentication software.

Read the entire Cyber Campaign Brief here.

New Malspam Campaign Delivers Adwind RAT – November 1, 2021

From October 22 to 27, Infoblox observed multiple related malspam campaigns distributing the remote access trojan (RAT) Adwind via weaponized Java and JavaScript files. Emails in these campaigns present themselves as coming from a logistics bureau, Al Bahr Al Arabi, and The United Bank of Egypt.

Adwind RAT is a cross-platform, multi-functional malware. It is openly distributed as a paid malware as a service (MaaS), which cyber criminals can customize and control.

Read the entire Cyber Campaign Brief here.

New Threat Actor: PINK BOA – November 2, 2021

Since the beginning of 2021, we have been tracking a threat actor, whom we have named PINK BOA. The actor has been highly active throughout this period, but the campaigns have intensified even further over the past several weeks.

PINK BOA uses a dictionary DGA (DDGA) algorithm to generate hostnames at random, and it uses thousands of IPs owned by the U.S.-based hosting provider Digital Ocean and spread out across the world. The results of a scan we performed on public reports suggest that most of the compromised IP addresses have vulnerabilities that can be exploited by remotely executing malicious code.

Read the entire Cyber Campaign Brief here.

Log4j Exploit Harvesting – December 13, 2021

On December 9, the National Institute of Standards and Technology disclosed a critical vulnerability in Log4j, which is a widely adopted logging software. This vulnerability is CVE-2021-44228, and it allows attackers to execute arbitrary code on a remote server. Because the vulnerability is easy to exploit, the global security industry immediately observed attackers in the wild and rapidly responded by identifying problems in software and mitigating risks. At the same time, attackers immediately began taking advantage of the vulnerability and have exploited systems worldwide.

We at Infoblox have observed multiple attacks via DNS; we are monitoring and updating our systems continuously. Out of an abundance of caution, we are adding all suspicious indicators to the blocklists for our customers.

Read the entire Cyber Campaign Brief here.

The Infoblox Threat Intelligence Group

With over 50 years of experience, the Infoblox Threat Intelligence Group creates, aggregates and curates information on threats to provide actionable intelligence that is high-quality, timely and reliable. Threat information from Infoblox filters out false positives and gives you the information you need to block the newest threats and to maintain a unified security policy across the entire security infrastructure of your organization.

Infoblox Threat Intelligence

Infoblox Threat Intelligence provides timely and accurate data that helps protect organizations against cyber threats. Our data is curated from more than two dozen partners, and our key sources include leading threat intelligence providers, government agencies, universities and the Department of Homeland Security's Automated Indicator Sharing program. Infoblox Threat Intelligence provides a single platform for managing and distributing all of our licensed data sets within an organization's ecosystem.

Powered by the
Infoblox Cyber Intelligence Group

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com