Infoblox

# Q1 | 2022 CYBER THREAT REPORT


Powered by the
**Infoblox Threat 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 Q1 2022 report includes information on threat intelligence reports that were published from January 1 to March 31, 2022.

We summarize important industry alerts, advisories and reports that the Infoblox Threat Intelligence Group (TIG), 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.

We put a special spotlight on using MITRE ATT&CK to clarify the DNS attack surface and how DNS security can address these threats directly.

We also spotlight the state of cyber security within South Asia. We have recently seen an attack upon Air India; the number of cyber attacks against the government and businesses in India has doubled in the past three years. We present a recent case study of the implementation of DNS security by an e-commerce leader in India.

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 Q1 2022, the Infoblox Threat Intelligence Group published the following reports that included extensive research on Ukrainian-themed campaigns:

- Cyber Threat Advisory: Formbook Deploys New Evasive Techniques
- Ukraine Scam Campaigns
- “Ukraine war” Malspam Delivers Remcos
- Ukraine-Themed Malspam Drops Agent Tesla
- Cyber Threat Advisory: Ukrainian Support Fraud

# Infoblox Threat Reports and Cyber Threat Alerts: Q1 2022

During Q1 2022, the Infoblox Threat Intelligence Group published the following reports on campaigns that delivered malware:

## Cyber Threat Advisory: Formbook Deploys New Evasive Techniques

March 31, 2022

On March 19, Infoblox observed a new spam campaign distributing Formbook infostealer malware through email attachments. Formbook is installed through two different droppers, which are usually associated with Agent Tesla – in fact, much of the delivery involves known tactics and techniques for Agent Tesla, but ultimately the payload in this campaign was Formbook. The droppers use VM detection, steganography, process hollowing, mutexes, and many other evasion techniques, and they rely heavily on XOR encryption.

At first glance, the characteristics of the campaign match those of campaigns known to distribute Agent Tesla and Formbook. Both are information stealers and capable of identifying and exfiltrating passwords from browsers, email clients, cryptocurrency wallets, and many other software applications. Both are sold as malware-as-a-service (MaaS) on specialized hacking forums, and both allow buyers to customize the malware with their own command and control (C&C) and obfuscation methods.

The spam lure is unsophisticated and has been used by threat actors consistently in recent years. All emails have the same subject line, “RE: Payment Transfer slip”, and a single attached file, Payment slip PDF.zip, which contains a PE32 executable called Payment Slip PDF.exe. Because the malware uses various anti-evasion and anti-detection techniques (described below), most antivirus solutions were unable to correctly identify the threat or to provide actionable intelligence.

View the full threat advisory here.

## Ukraine Scam Campaigns

March 25, 2022

During the weekend of March 19, Infoblox observed multiple email spam campaigns running scams and exploiting Russia’s invasion of Ukraine. War-related text appeared in the subject line or body of the emails. For reporting purposes, we have grouped these campaigns according to the following social-engineering tactics:

1. Baiting email recipients with giveaways of fake gift cards
2. 419 scam, which is also known as the Nigerian prince or the advance fee scam
3. Charity fraud

Many of these campaigns have been operating since early March. We have seen few changes in their message templates over the past couple of weeks. We suspect that the scam operators continue to reuse most of the message templates because they are effective.

Many of the spam campaigns described in the following sections began as early as March 8 and continue to operate at the time of this writing. We have observed three common social-engineering tactics across the campaigns: baiting with gift cards, the 419 scam and charity fraud.

The gift card scams exploit the names of famous retail brands and use buzzwords to tempt victims to click links to fraudulent landing pages, where the victims are prompted to fill out web forms with personal details. Notably, the URLs employ newly registered domains that are configured with mail exchange (MX) records and are used to send the spam emails.

The 419 group of scams claim to offer their targets the opportunity to earn commissions by handling transfers of large amounts of money. Usually, the sender of the scam email claims to be a government official; in the campaigns we have observed, the sender has provided a backstory about a Ukrainian father who died in the Russian invasion of Ukraine and left millions of dollars in inheritance.

Ukraine-related charity scams have been using a number of newly registered domains, and we have been tracking these scams since late February. The domains we observed during the weekend of March 19 were distributed via spam emails.

View the full cyber threat advisory here.

## "Ukraine war" Malspam Delivers Remcos

March 8, 2022

On March 2 and 3, Infoblox observed a malspam campaign that used messages related to Russia's invasion of Ukraine. This malspam campaign was attempting to lure users into opening an attached .xlsx file that downloads the Remcos remote access trojan (RAT). Infoblox has previously reported on malspam campaigns distributing Remcos.

We observed multiple Ukraine-related malspam campaigns within the first week after the invasion. Some of them distribute donation or cryptocurrency scams; others distribute malware, such as Remcos.

A German company called Breaking Security has been offering Remcos since 2016. One of the versions offered is free and has a limited number of features, and the other version is paid and starts at 58 euros. Although Remcos is marketed as a legitimate remote administration tool, it is frequently abused by threat actors and used for malicious purposes.

Breaking Security actively maintains and updates Remcos, with the latest update released on February 10. The capabilities of Remcos include remotely controlling infected computers, logging keystrokes and taking screenshots.

View the full cyber threat advisory here.

## Ukraine-Themed Malspam Drops Agent Tesla

February 4, 2022

On March 1, Infoblox observed a malspam campaign that was using messages related to Russia's invasion of Ukraine. The malspam campaign was trying to lure users into downloading a ZIP file attachment whose contents could download the Agent Tesla keylogger.

This campaign occurred a week after Russia invaded Ukraine. It is one of multiple campaigns that have taken advantage of the conflict by luring users via socially engineered emails and websites with look-alike domains that serve fake donation content.

Agent Tesla is a MaaS RAT that security researchers first discovered in 2014. It is usually distributed via spam or phishing emails, and it has many capabilities for stealing information from a victim's machine, including the following:

- Logging keystrokes
- Extracting data from the host's clipboard
- Capturing screens
- Grabbing forms
- Stealing credentials from VPN software

After gathering sensitive information from a victim's machine, Agent Tesla exfiltrates the stolen information by using a web browser or an email client.

View the full cyber threat advisory here.

## Cyber Threat Advisory: Ukrainian Support Fraud

February 2, 2022

Since the Russian invasion of Ukraine on February 24, the Infoblox Threat Intelligence Group has observed a marked increase in the number of new Ukraine-related domain names on our recursive DNS resolvers. Much of this activity is part of a global response to the humanitarian crisis happening in Eastern Europe, and some of this activity consists of new efforts led by previously uncoordinated groups. However, cyber criminals have also seized on the opportunity and created many sites to spoof or imitate genuine support efforts. Distinguishing between these two scenarios can be difficult even for the most cautious individuals.

Analysis of the DNS traffic over our recursive resolvers since February 24 has shown a dramatic increase in Ukraine-related domains: From February 24 to 28, over twice as many domains have been seen for the first time than in the week prior to the Russian offensive.

In response, Infoblox has developed multiple analytics and is actively assessing the threat level of newly observed domains. We have found indicators related to activities ranging from malware campaigns to individuals making new efforts to coordinate the delivery of medical supplies to Ukraine. Among the most prevalent threats in this environment are scams to collect cryptocurrency.

One of the developments that hinders analysis is that many efforts, both legitimate and fraudulent, are being established as Decentralized Anonymous Organizations (DAOs). A typical DAO is focused on a specific issue, such as the war in Ukraine, and is a member-owned organization without central leadership. These organizations rely on financial transaction records and rules established in a blockchain. In fact, on February 26 a Twitter account identifiable with the Ukrainian government requested cryptocurrency donations, which could have contributed to the flurry of emerging sites offering donations via virtual currency.

In the hours after Russian troops crossed the border with Ukraine, a number of legitimate DAOs were established to protest Russia's actions and create financial support for Ukraine. Perhaps most notable of these is Ukraine DAO, hosted on ukrainedao[.]love and established by Pussy Riot founder Nadya Tolokonnikova and other activists. Due to this DAO's new registration and use of cryptocurrency, many security vendors have falsely concluded that its hosting domain is malicious.

The website for Ukraine DAO offers two methods for donating to the cause: (1) individuals can donate cryptocurrency directly to the Ethereum wallet ukrainedao[.]eth, and (2) individuals with an on-chain wallet can donate and receive a "love" token that has no monetary value but does have social impact. Although hosted on a newly registered domain and using cryptocurrency, Ukraine DAO is publicly claimed by the founders and recognized in verified Twitter accounts. We have concluded that this domain is not hosting malware or fraudulent content.

View the full cyber threat advisory is here.

# Cybersecurity and Infrastructure Security Agency (CISA) Alerts in Q1 2022

### AA22-083A: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector

March 24, 2022

This joint Cybersecurity Advisory (CSA)—coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE)—provides information on multiple intrusion campaigns that were conducted by state-sponsored Russian cyber actors from 2011 to 2018 and that targeted U.S. and international organizations in the energy sector. CISA, the FBI, and DOE responded to these campaigns with appropriate action in and around the time they occurred. The agencies are sharing this information to highlight historical tactics, techniques, and procedures (TTPs) used by adversaries. Here are the excerpts:

On March 24, 2022, the U.S. Department of Justice unsealed indictments of three Russian Federal Security Service (FSB) officers and a Russian Federation Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) employee for their involvement in the following intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies.

- Global Energy Sector Intrusion Campaign, 2011 to 2018: the FSB conducted a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.
    - One of the indicted FSB officers was involved in campaign activity that involved deploying Havex malware to victim networks.
    - The other two indicted FSB officers were involved in activity targeting U.S. Energy Sector networks from 2016 through 2018.
- Compromise of Middle East-based Energy Sector organization with TRITON Malware, 2017: Russian cyber actors with ties to the TsNIIKhM gained access to and leveraged TRITON (also known as HatMan) malware to manipulate a foreign oil refinery's ICS controllers. TRITON was designed to specifically target Schneider Electric's Triconex Tricon safety systems and is capable of disrupting those systems. Schneider Electric has issued a patch to mitigate the risk of the TRITON malware's attack vector; however, network defenders should install the patch and remain vigilant against these threat actors' TTPs.
    - The indicted TsNIIKhM cyber actor is charged with attempting to access U.S. protected computer networks and to cause damage to an energy facility.
    - The indicted TsNIIKhM cyber actor was a co-conspirator in the deployment of the TRITON malware in 2017.

This CSA provides the TTPs used by indicted FSB and TsNIIKhM actors in cyber operations against the global Energy Sector. Specifically, this advisory maps TTPs used in the global Energy Sector campaign and the compromise of the Middle East-based Energy Sector organization to the MITRE ATT&CK for Enterprise and ATT&CK for ICS frameworks.

Click here for a PDF version of this report.

### AA22-076A: Strengthening Cybersecurity of SATCOM Network Providers and Customers

March 17, 2022

CISA and the FBI are aware of possible threats to U.S. and international satellite communication (SATCOM) networks. Successful intrusions into SATCOM networks could create risk in SATCOM network providers' customer environments.

Given the current geopolitical situation, CISA's Shields Up initiative requests that all organizations significantly lower their threshold for reporting and sharing indications of malicious cyber activity. To that end, CISA and FBI will update this joint CSA as new information becomes available so that SATCOM providers and their customers can take additional mitigation steps pertinent to their environments.

CISA and the FBI strongly encourage critical infrastructure organizations and other organizations that are either SATCOM network providers or customers to review and implement the mitigations outlined in this CSA to strengthen SATCOM network cybersecurity.

Click here for a PDF version of this report.

### AA22-074A: Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability

March 15, 2022

The FBI and CISA have issued a joint CSA to warn organizations that Russian state-sponsored threat actors have gained network access through exploitation of default Multi Factor Authentication (MFA) protocols.

As early as May 2021, Russian state-sponsored threat actors took advantage of a misconfigured account set to default MFA protocols at a non-governmental organization, allowing them to enroll a new device for MFA and access the victim network. The threat actors then exploited a critical Windows Print Spooler vulnerability, "PrintNightmare" (CVE-2021-34527) to run arbitrary code with system privileges. Russian state-sponsored cyber actors successfully exploited the vulnerability while targeting a non-governmental organization using Cisco's Duo MFA, enabling access to cloud and email accounts for document exfiltration.

The joint advisory provides observed tactics, techniques, and procedures, indicators of compromise (IOCs), and recommendations to protect against Russian state-sponsored malicious cyber activity. In the joint advisory FBI and CISA urge all


organizations to apply the recommendations in the Mitigations section of this advisory, including the following:

- Enforce MFA and review configuration policies to protect against "fail open" and re-enrollment scenarios.
- Ensure inactive accounts are disabled uniformly across the Active Directory and MFA systems.
- Patch all systems. Prioritize patching for known exploited vulnerabilities.

Click here for a PDF version of this report.

### AA21-291A: Destructive Malware Targeting Organizations in Ukraine

February 26, 2022 | Last revised: March 01, 2022

Leading up to Russia's unprovoked attack against Ukraine, threat actors deployed destructive malware against organizations in Ukraine to destroy computer systems and render them inoperable.

- On January 15, the Microsoft Threat Intelligence Center (MSTIC) disclosed that malware, known as WhisperGate, was being used to target organizations in Ukraine. According to Microsoft, WhisperGate is intended to be destructive and is designed to render targeted devices inoperable.
- On February 23, several cybersecurity researchers disclosed that malware known as HermeticWiper was being used against organizations in Ukraine. According to SentinelLabs, the malware targets Windows devices, manipulating the master boot record, which results in subsequent boot failure.

Destructive malware can present a direct threat to an organization's daily operations, impacting the availability of critical assets and data. Further disruptive cyberattacks against organizations in Ukraine are likely to occur and may unintentionally spill over to organizations in other countries. Organizations should increase vigilance and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event.

This joint CSA between CISA and the FBI provides information on WhisperGate and HermeticWiper malware as well as open-source IOCs for organizations to detect and prevent the malware. Additionally, this CSA provides recommended guidance and considerations for organizations to address as part of network architecture, security baseline, continuous monitoring, and incident response practices.

## AA21-291A: Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks

February 24, 2022

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 10. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

The FBI, CISA, the U.S. Cyber Command Cyber National Mission Force (CNMF), and the United Kingdom's National Cyber Security Centre (NCSC-UK) have observed a group of Iranian government-sponsored advanced persistent threat (APT) actors, known as MuddyWater, conducting cyber espionage and other malicious cyber operations targeting a range of government and private-sector organizations across sectors—including telecommunications, defense, local government, and oil and natural gas—in Asia, Africa, Europe, and North America. Note: MuddyWater is also known as Earth Vetala, MERCURY, Static Kitten, Seedworm, and TEMP.Zagros.

MuddyWater is a subordinate element within the Iranian Ministry of Intelligence and Security (MOIS). This APT group has conducted broad cyber campaigns in support of MOIS objectives since approximately 2018. MuddyWater actors are positioned both to provide stolen data and access to the Iranian government and to share these with other malicious cyber actors.

MuddyWater actors are known to exploit publicly reported vulnerabilities and use open-source tools and strategies to gain access to sensitive data on victims' systems and deploy ransomware. These actors also maintain persistence on victim networks via tactics such as side-loading dynamic link libraries (DLLs)—to trick legitimate programs into running malware—and obfuscating PowerShell scripts to hide C&C functions. FBI, CISA, CNMF, and NCSC-UK have observed MuddyWater actors recently using various malware—variants of PowGoop, Small Sieve, Canopy (also known as Starwhale), Mori, and POWERSTATS—along with other tools as part of their malicious activity.

This advisory provides observed TTPs; malware; and IOCs associated with this Iranian government-sponsored APT activity to aid organizations in the identification of malicious activity against sensitive networks.

The FBI, CISA, CNMF, NCSC-UK, and the National Security Agency (NSA) recommend organizations apply the mitigations in this advisory and review the following resources for additional information. Note: also see the Additional Resources section.

- Malware Analysis Report – MAR-10369127-1.v1: MuddyWater
- IOCs – AA22-052A.stix and MAR-10369127-1.v1.stix
- CISA's webpage – Iran Cyber Threat Overview and Advisories
- NCSC-UK MAR – Small Sieve
- CNMF's press release – Iranian intel cyber suite of malware uses open source tools

## AA22-054A: New Sandworm Malware Cyclops Blink Replaces VPNFilter

February 23, 2022

The UK's NCSC, CISA, NSA, and the FBI in the U.S. have identified that the actor known as Sandworm or Voodoo Bear is using a new malware, referred to here as Cyclops Blink. The NCSC, CISA, and the FBI have previously attributed the Sandworm actor to Russian GRU's Main Center for Special Technologies (GTsST). The malicious cyber activity below has previously been attributed to Sandworm:

- The BlackEnergy disruption of Ukrainian electricity in 2015
- Industroyer in 2016
- NotPetya in 2017
- Attacks against the Winter Olympics and Paralympics in 2018
- A series of disruptive attacks against Georgia in 2019

Cyclops Blink appears to be a replacement framework for the VPNFilter malware exposed in 2018, and which exploited network devices, primarily small office/home office (SOHO) routers and network attached storage (NAS) devices.

This advisory summarizes the VPNFilter malware it replaces, and provides more detail on Cyclops Blink, as well as the associated TTPs used by Sandworm. An NCSC malware analysis report on Cyclops Blink is also available.

It also provides mitigation measures to help organizations defend against malware.

## AA22-047A: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

February 16, 2022

From at least January 2020, through February 2022, the FBI, NSA, and CISA have observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resources. These CDCs support contracts for the U.S. Department of Defense (DoD) and Intelligence Community in the following areas:

- Command, control, communications, and combat systems;
- Intelligence, surveillance, reconnaissance, and targeting;
- Weapons and missile development;
- Vehicle and aircraft design; and
- Software development, data analytics, computers, and logistics.

Historically, Russian state-sponsored cyber actors have used common but effective tactics to gain access to target networks, including spearphishing, credential harvesting, brute force/password spray techniques, and known vulnerability exploitation against accounts and networks with weak security. These actors take advantage of simple passwords, unpatched systems, and unsuspecting employees to gain initial access before moving laterally through the network to establish persistence and exfiltrate data.

In many attempted compromises, these actors have employed similar tactics to gain access to enterprise and cloud networks, prioritizing their efforts against the widely used Microsoft 365 (M365) environment. The actors often maintain persistence by using legitimate credentials and a variety of malware when exfiltrating emails and data.

These continued intrusions have enabled the actors to acquire sensitive, unclassified information, as well as CDC-proprietary and export-controlled technology. The acquired information provides significant insight into U.S. weapons platforms development and deployment timelines, vehicle specifications, and plans for communications infrastructure and information technology. By acquiring proprietary internal documents and email communications, adversaries may be able to adjust their own military plans and priorities, hasten technological development efforts, inform foreign policymakers of U.S. intentions, and target potential sources for recruitment. Given the sensitivity of information widely available on unclassified CDC networks, the FBI, NSA, and CISA anticipate that Russian state-sponsored cyber actors will continue to target CDCs for U.S. defense information in the near future. These agencies encourage all CDCs to apply the recommended mitigations in this advisory, regardless of evidence of compromise.

For additional information on Russian state-sponsored cyber activity, see CISA's webpage, Russia Cyber Threat Overview and Advisories.

## AA22-040A: 2021 Trends Show Increased Globalized Threat of Ransomware

February 09, 2022 | Last revised: February 10, 2022

In 2021, cybersecurity authorities in the United States, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. The FBI, NSA, and CISA observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors. The Australian Cyber Security Center (ACSC) observed continued ransomware targeting of Australian critical infrastructure entities, including in the Healthcare and Medical, Financial Services and Markets, Higher Education and Research, and Energy Sectors. The NCSC recognizes ransomware as the biggest cyber threat facing the United Kingdom. Education is one of the top UK sectors targeted by ransomware actors, but the NCSC has also seen attacks targeting businesses, charities, the legal profession, and public services in the Local Government and Health Sectors.

Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally.

This joint Cybersecurity Advisory—authored by cybersecurity authorities in the United States, Australia, and the United Kingdom—provides observed behaviors and trends as well as mitigation recommendations to help network defenders reduce their risk of compromise by ransomware.

## AA22-011A: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

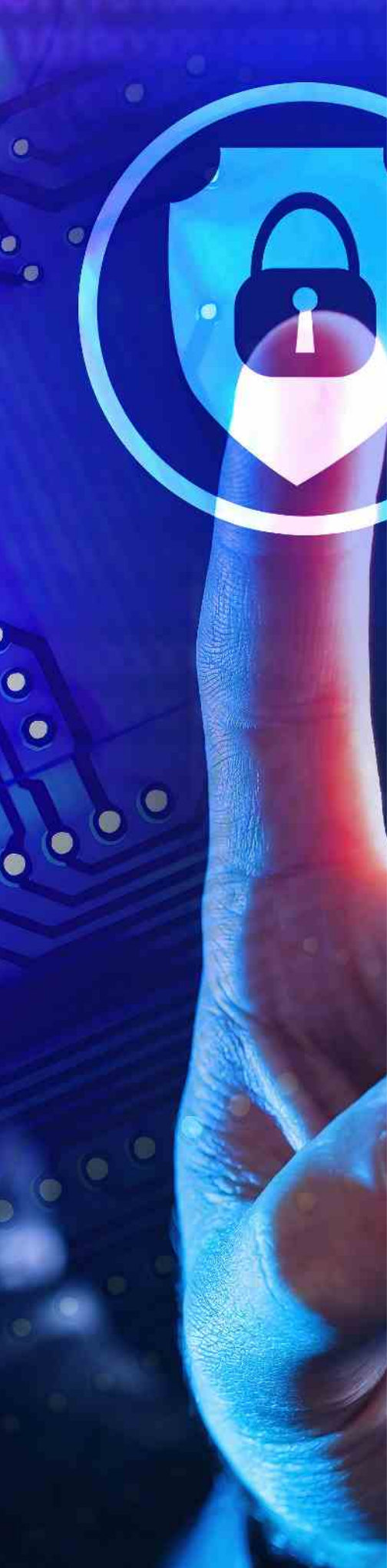
January 11, 2022 | Last revised: March 01, 2022

This joint CSA—authored by the FBI, NSA, and CISA—is part of a continuing cybersecurity mission to warn organizations of cyber threats and help the cybersecurity community reduce the risk presented by these threats. This CSA provides an overview of Russian state-sponsored cyber operations; commonly observed TTPs; detection actions; incident response guidance; and mitigations. This overview is intended to help the cybersecurity community reduce the risk presented by these threats.

CISA, the FBI, and NSA encourage the cybersecurity community—especially critical infrastructure network defenders—to adopt a heightened state of awareness and to conduct proactive threat hunting, as outlined in the Detection section. Additionally, CISA, the FBI, and NSA strongly urge network defenders to implement the recommendations listed below and detailed in the Mitigations section. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business degradation.

1. Be prepared. Confirm reporting processes and minimize personnel gaps in IT/OT security coverage. Create, maintain, and exercise a cyber incident response plan, resilience plan, and continuity of operations plan so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline.
2. Enhance your organization's cyber posture. Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.
3. Increase organizational vigilance. Stay current on reporting on this threat. Subscribe to CISA's mailing list and feeds to receive notifications when CISA releases information about a security topic or threat.

CISA, the FBI, and NSA encourage critical infrastructure organization leaders to review CISA Insights: Preparing for and Mitigating Potential Cyber Threats for information on reducing cyber threats to their organization.



# Federal Bureau of Investigation (FBI) IC3 Industry Alerts in Q1 2022

## Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector

March 25, 2022

Summary previously shown in the CISA Alerts section on page 9.

The complete Joint Cybersecurity Advisory can be viewed here.

## TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems

March 25, 2022

The FBI is warning that the group responsible for the deployment of TRITON malware against a Middle East–based petrochemical plant's safety instrumented system in 2017, the TsNIIKhM, continues to conduct activity targeting the global energy sector. This warning follows the 24 March 2022 unsealing of a US indictment of a Russian national and TsNIIkhM employee involved in that attack. TRITON was malware designed to cause physical safety systems to cease operating or to operate in an unsafe manner. Its potential impact could be similar to cyberattacks previously attributed to Russia that caused blackouts in Ukraine in 2015 and 2016. TRITON malware targeted the Schneider Electric Triconex safety instrumented system (SIS), which is used to initiate safe shutdown procedures in the event of an emergency. TRITON malware affected Triconex Tricon safety controllers by modifying in-memory firmware to add additional programming, potentially leading to damage of a facility, system downtime, and even loss of life should the SIS fail to initiate safe shutdown procedures. Schneider Electric addressed the vulnerability (with the Tricon model 3008 v10.0-10.4) when version 11.3 of the Tricon controller was released in June 2018; however, older versions of the controller remain in use and are vulnerable to a similar attack. As a result, the FBI is alerting the ICS community of continued activity by this group and requests that any indicators of potential compromise be reported to the FBI.

The complete Joint Cybersecurity Advisory can be viewed here.

## Indicators of Compromise Associated with AvosLocker Ransomware

March 18, 2022

AvosLocker is a ransomware-as-a-service (RaaS) affiliate-based group that has targeted victims across multiple critical infrastructure sectors in the United States including, but not limited to, the Financial Services, Critical Manufacturing, and Government Facilities sectors. AvosLocker claims to directly handle ransom negotiations, as well as the publishing and hosting of exfiltrated victim data after their affiliates infect targets. As a result, AvosLocker IOCs vary between indicators specific to AvosLocker malware and indicators specific to the individual affiliate responsible for the intrusion.

AvosLocker ransomware encrypts files on a victim's server and renames them with the ".avos" extension. AvosLocker actors then place ransom notes on the victim server and include a link to an AvosLocker .onion payment site. Depending upon the affiliate, payments in Monero are preferred; however, they accept Bitcoin for a 10-25% premium. We have also observed alleged AvosLocker representatives make phone calls to the victims to direct them to the payment site to negotiate. Multiple victims have also reported that AvosLocker negotiators have been willing to negotiate reduced ransom payments. The AvosLocker leak site claims to have targeted victims in the United States, Syria, Saudi Arabia, Germany, Spain, Belgium, Turkey, the United Arab Emirates, the United Kingdom, Canada, China, and Taiwan. The leak site includes samples of stolen victim data and threatens to sell the data to unspecified third parties, if a victim does not pay the ransom. AvosLocker ransomware is a multi-threaded Windows executable written in C++ that runs as a console application and shows a log of actions performed on victim systems. AvosLocker ransomware samples contained optional command line arguments that could be supplied by an attacker to enable/disable certain features.

The complete Joint Cybersecurity Advisory can be viewed here.

## Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability

March 16, 2022

Summary previously shown in the CISA Alerts section on page 14.

## RagnarLocker Ransomware Indicators of Compromise

February 7, 2022

The FBI first became aware of RagnarLocker in April 2020 and subsequently produced a FLASH to disseminate known IOCs at that time. This FLASH provides updated and additional IOCs to supplement that report. As of January 2022, the FBI has identified at least 52 entities across 10 critical infrastructure sectors affected by RagnarLocker ransomware, including entities in the critical manufacturing, energy, financial services, government, and information technology sectors. RagnarLocker ransomware actors work as part of a ransomware family, frequently changing obfuscation techniques to avoid detection and prevention.

RagnarLocker is identified by the extension ".RGNR_," which is a hash of the computer's NETBIOS name. The actors, identifying themselves as "RAGNAR_LOCKER," leave a .txt ransom note, with instructions on how to pay the ransom and decrypt the data. RagnarLocker uses VMProtect, UPX, and custom packing algorithms and deploys within an attacker's custom Windows XP virtual machine on a target's site.

Ragnar Locker uses Windows API GetLocaleInfoW to identify the location of the infected machine. If the victim location is identified as Azerbaijani, Armenian, Belorussian, Kazakh, Kyrgyz, Moldavian, Tajik, Russian, Turkmen, Uzbek, Ukrainian, or Georgian, the process terminates.

RagnarLocker checks for current infections to prevent multiple transform encryption of the data, potentially corrupting it. The binary gathers the unique machine GUID, operating system product name, and user name currently running the process. This data is sent through a custom hashing algorithm to generate a unique identifier.

RagnarLocker identifies all attached hard drives using Windows APIs: CreateFileW, DeviceIoControl, GetLogicalDrives, and SetVolumeMountPointA. The ransomware assigns a drive letter to any volumes not assigned a logical drive letter and makes them accessible. These newly attached volumes are later encrypted during the final stage of the binary.

RagnarLocker iterates through all running services and terminates services commonly used by managed service providers to remotely administer networks. The malware then attempts to silently delete all Volume Shadow Copies, preventing user recovery of encrypted files, using two different methods:

*>vssadmin delete shadows /all /quiet*

*>wmic.exe.shadowcopy.delete*

Lastly, RagnarLocker encrypts all available files of interest. Instead of choosing which files to encrypt, RagnarLocker chooses which folders it will not encrypt. Taking this approach allows the computer to continue to operate "normally" while the malware encrypts files with known and unknown extensions containing data of value to the victim.

## Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks

February 24, 2022

Summary previously shown in the CISA Alerts section on page 12.

## New Sandworm malware Cyclops Blink replaces VPNFilter

February 23, 2022

Summary previously shown in the CISA Alerts section on page 13.

## Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

February 17, 2022

Summary previously shown in the CISA Alerts section on page 14.

## Indicators of Compromise Associated with BlackByte Ransomware

February 11, 2022

This joint Cybersecurity Advisory was developed by the FBI and the U.S. Secret Service (USSS) to provide information on BlackByte ransomware. As of November 2021, BlackByte ransomware had compromised multiple US and foreign businesses, including entities in at least three U.S. critical infrastructure sectors (government facilities, financial, and food & agriculture). BlackByte is an RaaS group that encrypts files on compromised Windows host systems, including physical and virtual servers.

The BlackByte executable leaves a ransom note in all directories where encryption occurs. The ransom note includes the .onion site that contains instructions for paying the ransom and receiving a decryption key. Some victims reported the actors used a known Microsoft Exchange Server vulnerability as a means of gaining access to their networks. Once in, actors deploy tools to move laterally across the network and escalate privileges before exfiltrating and encrypting files. In some instances, BlackByte ransomware actors have only partially encrypted files. In cases where decryption is not possible, some data recovery can occur. Previous versions of BlackByte ransomware downloaded a .png file from IP addresses 185[.]93[.]6[.]31 and 45[.]9[.]148[.]114 prior to encryption. A newer version encrypts without communicating with any external IP addresses. BlackByte ransomware runs executables from c:\windows\system32\ and C:\Windows\. Process injection has been observed on processes it creates.

## 2021 Trends Show Increased Globalized Threat of Ransomware

February 9, 2022

Summary previously shown in the CISA Alerts section on page 15.

## Indicators of Compromise Associated with LockBit 2.0 Ransomware

February 4, 2022

LockBit 2.0 operates as an affiliate-based RaaS and employs a wide variety of TTPs, creating significant challenges for defense and mitigation. LockBit 2.0 ransomware compromises victim networks through a variety of techniques, including, but not limited to, purchased access, unpatched vulnerabilities, insider access, and zero day exploits. After compromising a victim network, LockBit 2.0 actors use publicly available tools such as Mimikatz to escalate privileges. The threat actors then use both publicly available and custom tools to exfiltrate data followed by encryption using the Lockbit malware. The actors always leave a ransom note in each affected directory within victim systems, which provides instructions on how to obtain the decryption software. The ransom note also threatens to leak exfiltrated victim data on the LockBit 2.0 leak site and demands a ransom to avoid these actions.

In July 2021, LockBit 2.0 released an update which featured the automatic encryption of devices across windows domains by abusing Active Directory group policies. In August 2021, LockBit 2.0 began to advertise for insiders to establish initial access into potential victim networks, while promising a portion of the proceeds from a successful attack. LockBit 2.0 also developed a Linux-based malware which takes advantage of vulnerabilities within VMWare ESXi virtual machines.


LockBit 2.0 is best described as a heavily obfuscated ransomware application leveraging bitwise operations to decode strings and load required modules to evade detection. Upon launch, LockBit 2.0 decodes the necessary strings and code to import the required modules followed by determining if the process has administrative privileges. If privileges are not sufficient, it attempts to escalate to the required privileges. Lockbit 2.0 then determines the system and user language settings and only targets those not matching a set list of languages that are Eastern European. If an Eastern European language is detected, the program exits without infection. As infection begins, Lockbit 2.0 deletes log files and shadow copies residing on disk. Lockbit 2.0 enumerates system information to include hostname, host configuration, domain information, local drive configuration, remote shares, and mounted external storage devices. Lockbit 2.0 attempts to encrypt any data saved to any local or remote device but skips files associated with core system functions. Once completed, Lockbit 2.0 deletes itself from disk and creates persistence at startup.

Prior to encryption, Lockbit affiliates primarily use the Stealbit application obtained directly from the Lockbit panel to exfiltrate specific file types. The desired file types can be configured by the affiliate to tailor the attack to the victim. The affiliate configures the application to target a desired file path and, upon execution, the tool copies the files to an attacker-controlled server using http. Due to the nature of the affiliate model, some attackers use other commercially available tools such as rclone and MEGAsync to achieve the same results. Lockbit 2.0 actors often use publicly available file sharing services including privatlab[.]net, anonfiles[.]com, sendspace[.]com, fex[.]net, transfer[.]sh, and send.exploit[.]in. While some of these applications and services can support legitimate purposes, they can also be used by threat actors to aid in system compromise or exploration of an enterprise.

## Potential for Malicious Cyber Activities to Disrupt the 2022 Beijing Winter Olympics and Paralympics

January 31, 2022

The FBI is warning entities associated with the February 2022 Beijing Winter Olympics and March 2022 Paralympics that cyber actors could use a broad range of cyber activities to disrupt these events. These activities include distributed denial of service (DDoS) attacks, ransomware, malware, social engineering, data theft or leaks, phishing campaigns, disinformation campaigns, or insider threats, and when successful, can block or disrupt the live broadcast of the event, steal or leak sensitive data, or impact public or private digital infrastructure supporting the Olympics. Additionally, the FBI warns Olympic participants and travelers of potential threats associated with mobile applications developed by untrusted vendors. The download and use of applications, including those required to participate or stay in the country, could increase the opportunity for cyber actors to steal personal information or install tracking tools, malicious code, or malware. The FBI urges all athletes to keep their personal cell phones at home and use a temporary phone while at the Games. The National Olympic Committees in some Western countries are also advising their athletes to leave personal devices at home or use temporary phones due to cybersecurity concerns at the Games. The FBI to date is not aware of any specific cyber threat against the Olympics, but encourages partners to remain vigilant and maintain best practices in their network and digital environments.

As we mentioned in PIN 20210719-001, large, high-profile events provide an opportunity for criminal and nation-state cyber actors to make money, sow confusion, increase their notoriety, discredit adversaries, and advance ideological goals. Due to the ongoing COVID-19 pandemic, no foreign spectators will be allowed to attend the Olympics or Paralympics. Spectators will be reliant on remote streaming services and social media throughout the duration of the Games. Adversaries could use social engineering and phishing campaigns leading up to and during the event to implant malware to disrupt networks broadcasting the event. Cyber actors could use ransomware or other malicious tools and services available for purchase to execute DDoS attacks against Internet service providers and television broadcast companies to interrupt service during the Olympics. Similarly, actors could target the networks of hotels, mass transit providers, ticketing services, event security infrastructure or similar Olympic support functions. For example, during the 2020 Tokyo Olympics and Paralympics, the NTT Corporation––which provided its services for the Tokyo Olympic & Paralympic Games––revealed there were more than 450 million attempted cyber-related incidents during the event, though none were successful due to cybersecurity measures in place. While there were no major cyber disruptions, the most popular attack methods used were malware, email spoofing, phishing and the use of fake websites and streaming services designed to look like official Olympic service providers. In addition, the use of new digital infrastructure and mobile applications, such as digital wallets or applications that track COVID testing or vaccination status, could also increase the opportunity for cyber actors to steal personal information or install tracking tools, malicious code, or malware. Athletes will be required to use the smartphone app, MY2022, which will be used to track the athletes' health and travel data. During the 2018 PyeongChang Winter Olympics, Russian cyber actors conducted a destructive cyber attack against the opening ceremony, enabled through spearphishing campaigns and malicious mobile applications.

## Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad

January 26, 2022

This Private Industry Notice provides a historical overview of Iran-based cyber company Emennet Pasargad's TTPs to enable recipients to identify and defend against the group's malicious cyber activities. On 20 October 2021, a grand jury in the U.S. District Court for the Southern District of New York indicted two Iranian nationals employed by Emennet Pasargad (formerly known as Eeleyanet Gostar) for computer intrusion, computer fraud, voter intimidation, interstate threats, and conspiracy offenses for their alleged participation in a multi-faceted campaign aimed at influencing and interfering with the 2020 U.S. Presidential Election. In addition, the Department of the Treasury Office of Foreign Assets Control designated Emennet along with four members of the company's management and the two indicted employees for attempting to influence the same election. The Department of State's Rewards for Justice Program also offered up to $10 million for information on the two indicted actors.

Starting in August 2020, Emennet Pasargad actors conducted a multi-faceted campaign to interfere in the 2020 U.S. Presidential Election. As part of this campaign, the actors obtained confidential U.S. voter information from at least one state election website; sent threatening email messages to intimidate voters; created and disseminated a video containing disinformation pertaining to purported but non-

existent voting vulnerabilities; attempted to access, without authorization, several states' voting-related websites; and successfully gained unauthorized access to a U.S. media company's computer network. During the 2020 election interference campaign, the actors claimed affiliation with the Proud Boys in the voter intimidation and disinformation aspects of the campaign. In addition to the 2020 U.S. election-focused operation in which the actors masqueraded as members of the Proud Boys, Emennet previously conducted cyber-enabled information operations, including operations that used a false-flag persona. According to FBI information, in late 2018, the group masqueraded as the "Yemen Cyber Army" and crafted messaging critical of Saudi Arabia. Emennet also demonstrated interest in leveraging bulk SMS services, likely as a means to mass-disseminate propaganda or other messaging. FBI information indicates Emennet poses a broader cybersecurity threat outside of information operations. Since 2018, Emennet has conducted traditional cyber exploitation activity targeting several sectors, including news, shipping, travel (hotels and airlines), oil and petrochemical, financial, and telecommunications, in the United States, Europe, and the Middle East.

The FBI is providing a summary of the group's past TTPs to recipients so they can better understand and defend against the group's future malicious activity. Emennet is known to use Virtual Private Network (VPN) services to obfuscate the origin of their activity. The group likely uses VPN services including TorGuard, CyberGhost, NordVPN, and Private Internet Access. Over the past three years, Emennet conducted reconnaissance and chose potential victims by performing web searches for leading businesses in various sectors such as "top American news sites." Emennet would then use these results to scan websites for vulnerable software that could be exploited to establish persistent access. In some instances, the objective may have been to exploit a large number of networks/websites in a particular sector as opposed to a specific organization target. In other situations, Emennet would also attempt to identify hosting/shared hosting services. After the initial reconnaissance phase, Emennet typically researched how to exploit specific software, including identifying open source available tools. In particular, Emennet demonstrated interest in identifying web pages running PHP code and identifying externally accessible mysql databases (in particular, phpMyAdmin).

Emennet also demonstrated an interest in exploiting the below software applications: Wordpress (in particular the revslider and layerslider plugins), Drupal, Apache, Tomcat, Ckeditor, and Fckeditor (including the exploitation of Roxy Fileman).

Emennet also expressed interest in numerous specific vulnerabilities, outlined in Appendix A of the original report. When conducting research, Emennet attempted to identify default passwords for particular applications a target may be using, and tried to identify admin and/or login pages associated with those same targeted websites. It should be assumed Emennet may attempt common plaintext passwords for any login sites they identify. Emennet is known to use the open source penetration testing tools SQLmap and the commercially available tool Acunetix during operational activity. They also likely use the below tools or resources:  DefenseCode, Web Security Scanner, Wappalyzer, DNS dumpster, Tiny mce scanner, Netsparker, Wordpress security scanner (wpscan), and Shodan. FBI information indicates the group has attempted to leverage cyber intrusions conducted by other actors for their own benefit. This includes searching for data hacked and leaked by other actors, and attempting to identify webshells that may have been placed or used by other cyber actors.

## Indicators of Compromise Associated with Diavol Ransomware

January 20, 2022

The FBI first learned of Diavol ransomware in October 2021. Diavol is associated with developers from the Trickbot Group, who are responsible for the Trickbot banking trojan. Diavol encrypts files solely using an RSA encryption key, and its code is capable of prioritizing file types to encrypt based on a pre-configured list of extensions defined by the attacker. While ransom demands have ranged from $10,000 to $500,000, Diavol actors have been willing to engage victims in ransom negotiations and accept lower payments. The FBI has not yet observed Diavol leak victim data, despite ransom notes including threats to leak stolen information.

Diavol creates a unique identifier for victim computers via the generation of a System or Bot ID with the following format:

*[hostname]-[username]_W[windows_version].[32CharacterString] (example BoT ID follows:)*

```
EXAMPLEHOSTNAME-EXAMPLEUSERNAME_W617601.6A8DA4GEEV11E43V85556FE984GG94W1G
```

The Bot ID generated by Diavol is nearly identical to the format used by TrickBot and the Anchor DNS malware, also attributed to Trickbot. Once the Bot ID is generated, Diavol attempts to connect to a hardcoded C&C address. If the registration to the botnet is successful, the infected device connects to the C&C again to request updated configuration values. Diavol encrypts files and appends the ".lock64" file extension to the encrypted files. The file contents are encrypted using Microsoft CryptoAPI functions and then written to the new encrypted file. Diavol can also terminate processes and services.

# National Security Agency/ Central Security Service (NSA-CSS) Advisories and Guidance Q1 2022

## CTR: Kubernetes Hardening Guidance

March 15, 2022 Update

Kubernetes® is an open-source system that automates the deployment, scaling, and management of applications run in containers, and is often hosted in a cloud environment. Using this type of virtualized infrastructure can provide several flexibility and security benefits compared to traditional, monolithic software platforms. However, securely managing everything from microservices to the underlying infrastructure introduces other complexities. This report is designed to help organizations handle Kubernetes-associated risks and enjoy the benefits of using this technology.

## CSA: Conti Ransomware

March 9, 2022 Update

Conti cyber threat actors remain active and reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1000. Notable attack vectors include Trickbot and Cobalt Strike (see original report for details). While there are no specific or credible cyber threats to the U.S. homeland at this time, CISA, FBI, NSA, and USSS encourage organizations to review this advisory and apply the recommended mitigations. CISA and the FBI have observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and workstations, and demand a ransom payment.

## CTR: Network Infrastructure Security Guidance

March 1, 2022

Guidance for securing networks continues to evolve as new vulnerabilities are exploited by adversaries, new security features are implemented, and new methods of securing devices are identified. Improper configuration, incorrect handling of configurations, and weak encryption keys can expose vulnerabilities in the entire network. All networks are at risk of compromise, especially if devices are not properly configured and maintained. An administrator's role is critical to securing the network against adversarial techniques and requires dedicated people to secure the devices, applications, and information on the network. This report presents best practices for overall network security and protection of individual network devices, and will assist administrators in preventing an adversary from exploiting their network.

## CAS: Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks

February 24, 2022

Summary previously shown in the CISA Alerts section on page 12.

## CSA: New Sandworm malware Cyclops Blink replaces VPNFilter

February 23, 2022

Summary previously shown in the CISA Alerts section on page 13.

## CSI: Cisco Password Types: Best Practices

February 17, 2022

Three years ago, the DHS released an alert on how cyber adversaries obtained hashed password values and other sensitive information from network infrastructure configuration files. Once the hashes were obtained, the adversaries were able to compromise network devices. That alert showed the results of what happens when cyber adversaries compromise device configurations that have insecure, reversible hashes: they are able to extract sensitive information and compromise networks. The rise in the number of compromises of network infrastructures in recent years is a reminder that authentication to network devices is an important consideration. Network devices could be compromised due to: poor password choice (vulnerable to brute force password spraying), router configuration files (which contain hashed passwords) sent via unencrypted email, or reused passwords (where passwords recovered from a compromised device can then be used to compromise other devices). Using passwords by themselves increases the risk of device exploitation. While NSA strongly recommends multi-factor authentication for administrators managing critical devices, sometimes passwords alone must be used. Choosing good password storage algorithms can make exploitation much more difficult.

## CSA: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

February 16, 2022

From at least January 2020, through February 2022, the FBI, NSA, and CISA have observed regular targeting of U.S. CDCs by Russian state-sponsored cyber actors. The actors have targeted both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resources. These CDCs support contracts for the DoD and the Intelligence Community in the following areas:

- Command, control, communications, and combat systems;
- Intelligence, surveillance, reconnaissance, and targeting;
- Weapons and missile development;
- Vehicle and aircraft design; and
- Software development, data analytics, computers, and logistics.

Historically, Russian state-sponsored cyber actors have used common but effective tactics to gain access to target networks, including spearphishing, credential harvesting, brute force/password spray techniques, and known vulnerability exploitation against accounts and networks with weak security. These actors take advantage of simple passwords, unpatched systems, and unsuspecting employees to gain initial access before moving laterally through the network to establish persistence and exfiltrate data.

## CSA: 2021 Trends Show Increased Globalized Threat of Ransomware

February 9, 2022

Summary previously shown in the CISA Alerts section on page 15.

## 2021 NSA Cybersecurity Year in Review

February 3, 2022

NSA formed a Cybersecurity Directorate in 2019 with the charge to prevent and eradicate threats to the United States' National Security Systems and critical infrastructure, with an initial focus on the Defense Industrial Base and its service providers. Drawing on NSA's rich information assurance legacy, the Cybersecurity Directorate refocused to meet the demands of the present and the future. It integrated key parts of NSA's cybersecurity mission such as threat intelligence, vulnerability analysis, cryptographic expertise and defensive operations into a more public-facing organization determined to raise the cybersecurity bar across government and industry while also imposing cost on U.S. adversaries. While much of the critical work that NSA does to secure the nation cannot be publicly disclosed, this year in review shares a wealth of information on cybersecurity efforts that have better equipped the U.S. to defend against the highest priority cyber threats from November 1, 2020 through October 31, 2021. Visit NSA.gov/cybersecurity to access the report digitally. Provide NSA Cybersecurity with feedback or ask questions by emailing cybersecurity@nsa.gov.

## CSA: Protecting VSAT Communications

January 25, 2022

Commercial Very Small Aperture Terminal (VSAT) networks are increasingly used for remote communications in support of U.S. government missions. Due to the nature of VSAT network communication links and recent vulnerabilities discovered in VSAT terminals, network communications over these links are at risk of being exposed and may be targeted by adversaries for the sensitive information they contain or to compromise connected networks. Most of these links are unencrypted, relying on frequency separation or predictable frequency hopping rather than encryption to separate communications. Public vulnerability research has found certain terminal equipment vulnerable to compromise and illicit firmware modification. NSA recommends that VSAT networks enable any available transmission security (TRANSEC) protections, segment and encrypt network communications before transmitting across the VSAT links, and keep VSAT equipment and firmware up to date.

## CTR: Recommendations for Configuring Adobe Acrobat Reader DC in a Windows Environment

January 20, 2022

Malicious cyber actors have a long and well-documented history of targeting users (including Department of Defense and National Security Systems) using malicious Portable Document Files (PDFs). However, modern security features for sandboxing and access control can help constrain what malicious PDFs can do, and can be rolled out en masse, limiting this common access vector at scale. This configuration guide provides recommendations on configuring Adobe Acrobat® Reader® DC in a Windows® environment. Administrators operating in a typical environment where Acrobat Reader is used solely for viewing PDF documents may use the Appendix: Configuring Settings for Adobe's Acrobat Reader DC as a quick guide to configure the Adobe Customization Wizard with the recommendations suited to their environment. The recommendations flagged in the Appendix as "always" are sufficient for most environments and are suitable for security compliance checklists. In some situations, however, users may utilize features of Adobe's Acrobat Reader requiring scripting or data sharing. In these cases, administrators should carefully review this configuration guide to select configuration options that will have minimal impact on usability while providing the most protection.

## CSA: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

January 11, 2022

Summary previously shown in the CISA Alerts section on page 16.

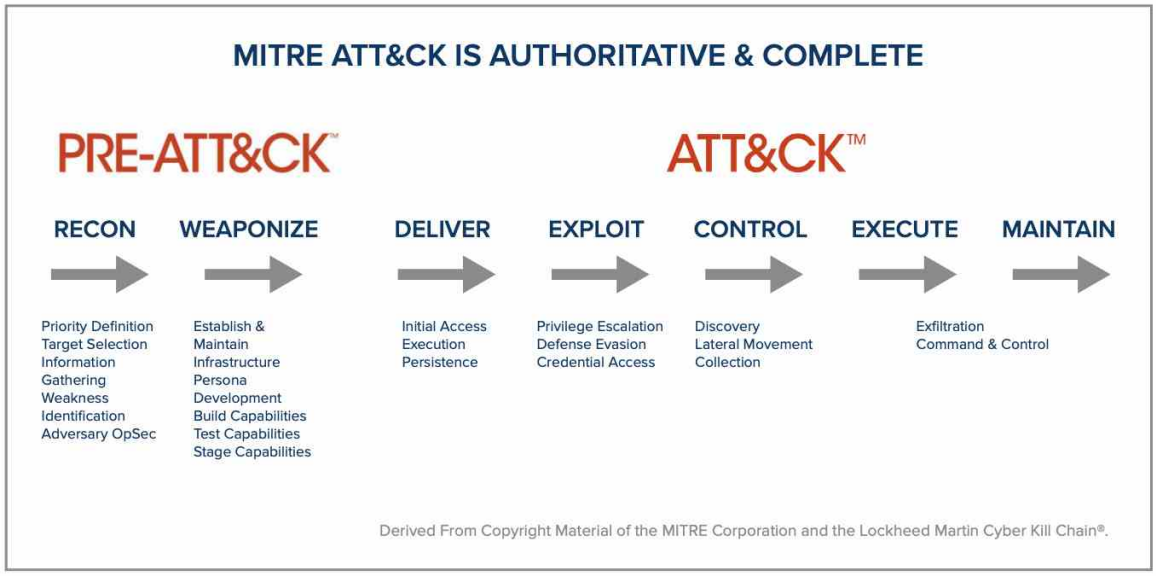
# Spotlight on MITRE ATT&CK: Understanding the DNS Attack Surface

This section will overview the MITRE ATT&CK® framework and why it is compelling for modern enterprise and government institutions. We discuss how leaving DNS unprotected exposes a large, accessible, and highly vulnerable attack surface. We illustrate this vulnerability gap by defining the MITRE ATT&CK Tactics, Techniques (and sub-techniques) and Procedures (TTPs) that use DNS. BloxOne® Threat Defense DNS security can protect against a multitude of techniques used by cyber attackers.

## The MITRE ATT&CK Framework

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework was developed and released by the MITRE Corporation in 2015. It is a comprehensive knowledge base of cyber attacker TTPs gathered from the observation of attacker behavior. MITRE is a non-profit organization that works with U.S. government agencies in a wide variety of areas.

As an important knowledge base, MITRE ATT&CK enables anyone on a cyber defense team to review and contrast attacker activity and then understand the best options for defense. In addition, there is also MITRE PRE-ATT&CK, which helps cyber defenders prevent an attack before the attacker can gain access to the network. The 15 top-level tactic categories of PRE-ATT&CK correlate to the first two stages of the Lockheed Martin Cyber Kill Chain®. PRE-ATT&CK presents the TTPs that a cyber attacker will use to define targets, gather information and then launch an attack.



MITRE ATT&CK introduced a lexicon that is now in common use and describes the activities of cyber attackers and the step-by-step tactics and techniques they use. This lexicon enables researchers to communicate clearly on the exact details of a threat.

MITRE ATT&CK provides a consistent method for describing current security controls and processes. This allows cyber defenders to clearly identify the nature of a threat, map that threat back to the controls that should protect against it and then ultimately determine whether that control is effective.

The MITRE ATT&CK framework supplies a comprehensive taxonomy to post-exploitation behavior of cyber attackers. The framework-provides detailed insight into attacker behavior and can be the best way to find and stop an ongoing attack before data exfiltration or destructive behavior can occur. MITRE ATT&CK can help organizations make better decisions about assessing risks, deploying new security controls and defending networks. Security solutions have begun to integrate the MITRE ATT&CK framework into their solutions as well, helping researchers map security information and events coming from these solutions to the framework.

## Mapping the DNS Attack Surface with MITRE ATT&CK

Everything on your networks—whether on premises, in the Cloud, Internet of Things (IoT) or mobile—will need to use DNS services. DNS provides centralized visibility and control of all computing resources, including users and servers in a micro-segment, all the way to an individual IP address. Cyber attackers can leverage unprotected DNS services in many ways.

Under the ATT&CK framework, a tactic is the goal an attacker is trying to achieve, and the techniques and sub-techniques are the ways of achieving that goal. Mitigation of these techniques and sub-techniques requires comprehensive DNS security solutions. The following MITRE ATT&CK techniques and sub-techniques explicitly define how cyber attackers will target and use DNS services.

**“MITRE ATT&CK has broken down the structure of attacks in a very consistent way that makes it straightforward to compare them and then determine how an attacker might have exploited the targeted network. Attacker analysis primarily focuses on their activities in terms of perimeter defense. MITRE ATT&CK takes a very focused look at attackers once they get in.”**

*Anthony James*
*Vice President of Product Marketing*
*Infoblox*

## MITRE ATT&CK Techniques That Use DNS

| TACTIC GOAL OF ATTACKER | TECHNIQUES USING DNS | SUB-TECHNIQUE |
|---|---|---|
| Reconnaissance | T1590 Gather Victim Network Information | .001 Domain Properties |
| | | .002 DNS |
| | | .004 Network Topology |
| | | .005 IP Address |
| | T1598 Phishing for Information | .003 Spearphishing Link |
| Resource Development | T1583 Acquire Infrastructure | .001 Domains |
| | | .002 DNS Server |
| | T1584 Compromise Infrastructure | .001 Domains |
| | | .002 DNS Server |
| | T1608 Stage Capabilities | .002 Upload Tool |
| Initial Access | T1189 Drive-by Compromise | |
| | T1190 Exploit Public-Facing Application | |
| | T1566 Phishing | .002 Spearphishing Link |
| Execution | T1204 User Execution | .001 Malicious Link |
| Credential Access | T1557 Adversary-in-the-Middle | |
| | T1040 Network Sniffing | |
| Command and Control | T1071 Application Layer Protocol | .004 DNS |
| | T1132 Data Encoding | |
| | T1568 Dynamic Resolution | |
| | T1573 Encrypted Channel | |
| | T1008 Fallback Channels | |
| | T1105 Ingress  Tool Transfer | |
| | T1572 Protocol Tunneling | |
| | T1090 Proxy | .001 Internal Proxy |
| | | .002 External Proxy |
| Exfiltration | T1030 Data Transfer Size Limits | |
| | T1048 Exfiltration Over Alternative Protocol | .001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol |
| | | .002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol |
| | | .003 Exfiltration Over Unencrypted Obfuscated Non-C2 Protocol |
| | T1041 Exfiltration Over C2 Channel | |

Let's take a close look at the Reconnaissance tactic: gathering information that can be used to plan future attacks. MITRE ATT&CK defines two techniques (and multiple sub-techniques) that attackers employ extensively to use DNS:

- **T1590: Gathering Victim Network Information**

  Information might include administrative data (such as IP ranges and domain names) and specifics about the network's topology and operations.

  - **.001 Domain Properties:** Information might include the domain(s) the victim owns, administrative data (such as names and registrars) and more directly actionable information, such as contacts (email addresses and phone numbers), business addresses and name servers.
  - **.002 DNS:** DNS information might include registered name servers and the records that outline addressing for a target's subdomains, mail servers and other hosts.
  - **.004 Network Topology:** Information might include the physical and/or logical arrangement of both external-facing and internal network environments. This information might also cover specifics about network devices (such as gateways and routers) and other infrastructure.
  - **.005 IP Addresses:** Public IP addresses might be allocated to organizations by block or as a range of sequential addresses; adversaries might attempt to determine which IP addresses are in use. IP addresses can enable an adversary to derive other details about a victim, such as the size of the victim's organization, the victim's physical location(s), the internet service provider and/or where and how the victim's publicly-facing infrastructure is hosted.

- **T1598: Phishing for Information**

  Adversaries send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information attempts to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from phishing in a general sense: the objective of the former is to gather data from the victim, but the objective of the latter is to execute malicious code.

  .003 Spear Phishing Link: Adversaries might send spear phishing messages with a malicious link, to elicit sensitive information that can be used during targeting. Spear phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spear phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (such as Establish Accounts or Compromise Accounts) and/or sending multiple, seemingly urgent messages.

All of these MITRE ATT&CK–DNS-related techniques and sub-techniques define areas of potential risk for your organization. If your DNS, DHCP and IPAM infrastructure is undefended, attackers will quickly discover and utilize these areas.

## Infoblox BloxOne Threat Defense

BloxOne Threat Defense brings all of your DNS controls, administration and management into one hybrid architecture. BloxOne Threat Defense gives you one architecturally efficient, centralized point of control and visibility to any traffic that requires resolution of a domain name with DNS services for all of your on-premises and cloud-based resources, including remote workers and their devices. Once you assert this control, you have very effectively enabled the defensive build-out of DNS. BloxOne Threat Defense secures traditional networks, as well as SD-WAN, IoT, the Cloud and the move to mobile devices.

It is a fact that most malware and advanced threats must rely on the use or compromise of DNS to execute and complete their attack successfully, and DNS can often be used to avoid detection by standard security tools. BloxOne Threat Defense will close this security gap and can enhance the  rest of the security ecosystem to strengthen defenses against sophisticated threats.

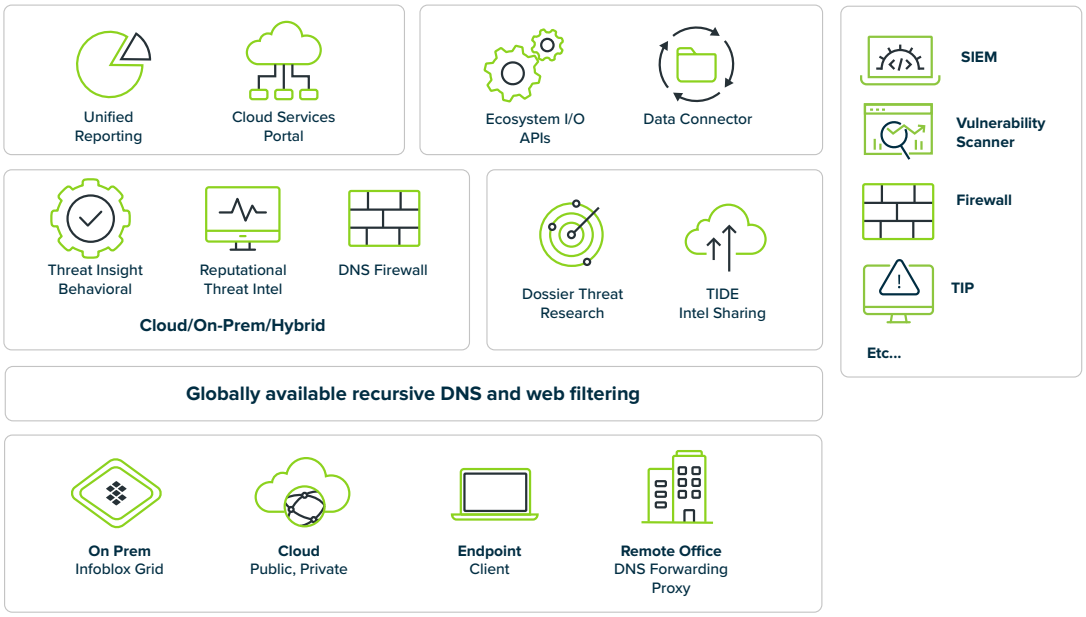
DNS security works at the ground level—that's why we say it is foundational. It is designed to prevent users or devices from connecting to malicious destinations, and to detect anomalous behaviors in the network such as C&C communications, advanced persistent threat activity, domain generation algorithm (DGA) activity, botnet communications, DNS tunneling, and data exfiltration, and more.

In addition, Infoblox DNS security integrates with Security Orchestration Automation and Remediation (SOAR) systems, ITSM solutions, vulnerability scanners and other tools in your security ecosystem to trigger remediation actions automatically when any malicious activity is detected. These integration and automation capabilities can dramatically speed an organization's threat investigation and incident response to security events.

Analyzing DNS logs is a highly effective way to see what resources a client has been accessing historically. DHCP fingerprint and IPAM metadata provide contextual information on compromised devices, such as the type of a device, the OS information, the network location and the current and historical IP address allocations. All this information helps with event correlation and understanding the scope of a breach.

BloxOne Threat Defense also combines advanced analytics based on machine learning, highly accurate and aggregated threat intelligence and automation to detect and prevent a broad range of threats. These threats may include DGAs, data exfiltration, look-alike domain use, fast flux and many others.

## BloxOne® Threat Defense




## Summary

MITRE ATT&CK is an important tool for identifying, analyzing and communicating consistently about malicious cyber activity. A multitude of attacker vectors identified within MITRE ATT&CK use and impact DNS. Core network services, such as DNS, DHCP and IPAM, provide deep visibility and can help organizations rapidly investigate a threat or anomalous behavior and share valuable data with the rest of the security ecosystem. Using DNS security and leveraging DNS-related data can reduce risk for every cloud, hybrid and on-premises resource that your organization depends on for success.

# Spotlight on South Asia: E-Commerce Leader in India Implements DNS Security

## State of the India Cyber Threat Landscape

In February 2022, IndiaTimes.com noted that, according to the research conducted at University of Surrey, attacks on businesses and government in India have doubled in the past three years. The number of successful cyber attacks in India has been growing almost on a monthly basis. In 2020, as per the FBI IC3 Internet Crime Report, India ranked approximately fourth among the top 20 countries being victimized by cyber crimes. In 2021, India recorded well over 3,000 victims of cybercrimes, right behind the United States, United Kingdom, and Canada, which rank first, second, and third, respectively.

As in the rest of the world, the drivers for much of this increase in India are the ongoing digital transformation, the growth in the use of mobile and IoT devices, and the increase in remote work associated with the COVID19 pandemic. These factors have increased the available attack surface across all of IT. Since the beginning of the pandemic, organizations in India have seen a 4,000-percent increase in the number of phishing emails. Approximately two-thirds of these same organizations have fallen victim to cyber attacks since shifting to a remote work model. In some cases, as in the attack on the power grid supplying Mumbai, cyber attacks are politically motivated.

Cyber attack activity has driven the Indian cyber security services and products to a total of $9.85 billion in revenue in 2021. Cyber security services industry grew from $4.3 billion in 2019 to $8.48 billion in 2021, and this represents a cumulative average growth rate of 40.33 percent. Almost in lockstep, the cybersecurity products industry grew from just $740 million in 2019 to $1.37 billion in 2021, and this represents another very high cumulative average growth rate of 36.49 percent. In roughly the same time period, India's cyber security workforce grew from approximately 110,000 employees in 2019 to over 218,000 in 2021.

In February 2022, Air India experienced a major cyber attack that compromised approximately 4.5 million customer records. Passport, ticket, and some credit card information was compromised. The breach involved all information registered between August 26, 2011, and February 20, 2021.

A high-profile India-based payment company, Juspay, suffered a data breach impacting 35 million customers. This breach was announced in early 2021 but happened approximately five months earlier, in 2020. This breach is very noteworthy because Juspay handles payments for online marketplaces, including Amazon and other big players. Data breached and released on the dark web and made available for purchase included credit card information and fingerprint scans.

In 2020, approximately 82% of Indian companies suffered ransomware attacks. In 2021, the impact of ransomware activity in India drove the cost of recovery from approximately $1.1 million in 2020 to $3.38 million in 2021. According to official estimates, in 2021, ransomware attacks increased by 120 percent.

Even government agencies with the highest levels of cyber protection are not exempt from the barrage of attacks. In 2021, the personally identifiable information (PII)—names, mobile phone numbers, emails, dates of birth, and more—of over 500,000 Indian police personnel went up for sale on the dark web.

**India-Based E-Commerce Leader Selects Infoblox for DNS Security**

This unidentified e-commerce leader has online sales, marketing and fulfillment operations across India and other countries in South Asia. It sells many different categories of products and has grown organically and through acquisition, and its broad network of modern distribution facilities serves millions of users. This company selected Infoblox BloxOne Threat Defense to address vulnerabilities and protect it and its customers. BloxOne Threat Defense is part of an expanded cyber security strategy for advanced threat intelligence and prevention of DNS-based data exfiltration. The e-commerce leader can now globally leverage the full set of BloxOne foundational security capabilities for expanded protection, both on-premises and within the cloud.

This South Asian e-commerce business, like many e-commerce companies, has been under continuous attacks. Global threat actors large and small have attempted to compromise the company's operations, divert funds and shipments of goods and exfiltrate proprietary corporate and customer information. The actors have used passwords acquired during the breach of a business associate's device to compromise the account holders of this e-commerce leader. This incident raised concern in the industry and brought to the fore the importance of increasing the resiliency of a company's DNS cyber defenses.

The goals of the DNS security acquisition included the need for additional control over access management, to identify and stop DNS tunneling attacks, deeper insight into user activity, more threat intelligence data and safer accommodation for work from home. During the ongoing pandemic, work from home requirements have been very important. This company chose to enhance technology and cyber security by making significant investments in improving defenses and reducing vulnerabilities. The protection of critical DNS assets became a core part of the company's cyber defense strategy.

This e-commerce leader has a complex technology and network environment, and this required API-level integration with the chosen DNS solution. This environment includes:

- Endpoint Security (XDR)
- Integrated Ticket Management System
- Data Loss Prevention (DLP)
- Cloud Access Security Broker (CASB)
- Identity Access Management (IAM)
- Threat Intelligence Tools and Feeds

- Next-Generation Firewall (NGFW)
- Virtual Private Network (VPN)
- Microsoft Office 365, Azure
- Internet Monitoring

Important DNS security use cases had to be addressed. These included malware detection and protection, data exfiltration, user visibility and look-alike domains.

The company selected, acquired and installed Infoblox BloxOne Threat Defense because it provides the enhanced visibility needed to detect and prevent DNS-based data exfiltration and address the other critical use cases. DNS servers normally use port 53 to listen for queries from DNS clients. Our team demonstrated how we connect and show data exfiltration through port 53; namely, we connected to the client's network and demonstrated how a threat actor could easily acquire documents and other information.

This e-commerce leader looked to the future expansion of its IT operations and felt that our support for Chrome OS and Linux was essential to its operations in India. We also provided a path to Cloud-based DDI services that can be integrated with the DNS security platform.

# 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 Threat Intelligence Group**



Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com



Infoblox