DXC.technology

Security Threat Intelligence Report

July-August 2020

In this issue

About this report

Fusing a range of public and proprietary information feeds, including DXC's global network of security operations centers and cyber intelligence services, this report delivers an overview of major incidents, insights into key trends and strategic threat awareness.

This report is a part of **DXC Labs | Security**, which provides insights and thought leadership to the security industry.

Intelligence cutoff date:
July 31, 2020

Message from Mark Hughes

Each month, we report on ransomware attacks, and DXC is not immune. Our Xchanging subsidiary was attacked in July. While the incident was contained within days with minimal impact on customers and no loss of data, the attack underscores the prevalence of evolving ransomware threats. Elsewhere, various families of ransomware are attacking Windows- and Linux-based systems with destructive effect. In addition, new remote code execution (RCE) vulnerabilities have surfaced. In today's environment, we all need to stay focused on securing infrastructure and data, increasing awareness and reducing the number of exposed threat vectors.

Mark Hughes
Senior Vice President and General Manager of Security
DXC Technology

Table of contents

Threat Updates

Vulnerability Updates

Incidents/breaches

Nation State and Geopolitical

7K

North Korean leader Kim Jong Un has quietly built a 7,000-man cyber army trained to find secrets, disrupt critical infrastructure and steal money.

2.3

Amazon Web Services (AWS) was able to hold off a record-setting distributed denial-of-service (DDOS) attack in February 2020 that fired 2.3 terabytes per second of network traffic at AWS.

12M

A South African bank is replacing 12 million cards after employees stole a master key and used it to steal $3.2 million.

100K

Brute-force attacks against the Windows Remote Desktop Services have almost doubled in the shift to remote working during the pandemic, reaching 100,000 attacks daily.

Threat Updates

HIDDEN COBRA adds 3 new tools

The U.S. Department of Homeland Security (DHS), Department of Defense (DoD) and the Federal Bureau of Investigation (FBI) released three new malware analysis reports covering three new tools related to North Korean threat actor HIDDEN COBRA (aka Lazarus Group, APT38):

- **COPPERHEDGE**, a full-featured remote access tool capable of running arbitrary commands, performing system reconnaissance and exfiltrating data
- **TAINTEDSCRIBE**, a full-featured beaconing implant, including its command modules. A beacon is a malicious agent/implant on a compromised system that calls back to the attacker-controlled system and checks for any new commands that should be executed. The main executable disguises itself as Microsoft Narrator, which downloads its command execution module from a command and control (C2) server. Capabilities include:
  - Download, upload, delete and execute files
  - Enable Windows CLI access, create and terminate processes
  - Perform target system enumeration
- **PEBBLEDASH** is a full-featured beaconing implant. This sample uses FakeTLS (Transport Layer Security) for session authentication and for network encoding utilizing Rivest Cipher 4 (RC4) encryption to obfuscate its network communications. Capabilities include:
  - Download, upload, delete and execute files
  - Enable Windows CLI access
  - Create and terminate processes
  - Perform target system enumeration

Impact

The new tools documented above will allow HIDDEN COBRA to expand attacks. Past behavior indicates the group develops new tools to adapt to advances in security controls. New tool development is normally followed by an increase in malicious group activity against multiple targets in various industry sectors.

The new tools expand the group's ability to perform malicious tasks including remote system takeover, exfiltration of sensitive data and installing spyware on targeted systems for espionage activities.

DXC perspective

HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims. The group is financially motivated; however, intrusions have also resulted in the exfiltration of data or system wiping.

The group is well funded and has the skill set to develop, maintain and deploy a wide range of tools. The recent addition of the described tools will require security teams to tune security monitoring tools to detect intrusions by this group, as well as hunt for its existing presence on networks.

Source: Department of Homeland Security/CISA/FBI

Tycoon ransomware targets Windows and Linux machines

BlackBerry Research/KPMG intelligence and incident response teams recently discovered this new ransomware strain written in Java that locked out system administrators following an attack on the organization's domain controller and file servers.

Tycoon was developed to avoid detection and to work on both Windows and Linux operating systems. Forensics showed the initial intrusion occurred through an internet-facing RDP jump-server and deployed the ransomware in a Trojanized Java Runtime Environment (JRE) and leveraged an obscure Java image format.

Tycoon ransomware comes in form of a ZIP archive containing the Trojanized Java Runtime Environment (JRE) build. The malware is compiled into a Java image file (JIMAGE) located at lib\modules within the build directory. JIMAGE is a special file format that stores custom JRE images designed to be used by the Java Virtual Machine (JVM) at runtime. Unlike the popular Java Archive format (JAR), JIMAGE is mostly internal to the JDK and rarely used by developers.

Tycoon ransomware encompasses resources and class files of all Java modules that support the specific JRE build. The format was first introduced in Java version 9 and is sparsely documented. The OpenJDK9 JIMAGE utility can extract and decompile Java image files. After extraction, the ransomware image contains three modules related to a project called "Tycoon."

Impact

Researchers analyzed a malware sample found on Windows systems and have discovered that the JRE build contains Linux scripts as well. The scripts in both platforms run the main function of the malicious Java module, which executes the ransomware.

This malware also has a persistence mechanism built-in, using a technique called Image File Execution Options (IFEO) injection. IFEO settings are stored in the Windows registry.

This persistence, combined with a highly targeted delivery system, means the malware has a high chance of being executed on a system without detection.

DXC perspective

The threat actors initially targeted small- to midsize businesses, knowing that cyber defenses and budgets in this sector are limited; however, the initial targets may have been used to test the effectiveness of the malware.

Large organizations should monitor for Tycoon activity in their environments as well. This malware appears to be in a development phase and highly sophisticated. Threat actors behind this campaign will be motivated to capitalize on their investment by focusing on targets with larger financial resources.

Organizations should consider securing external-facing servers and implementing a privileged access management solution and endpoint protection that detects and stops abnormal behavior.

Primary defenses against ransomware center on preventing it from infecting systems or spreading through the network.

Organizations should consider the following:

- Educating users on spotting potential phishing emails and the dangers associated with clicking links and attachments in unsolicited emails
- Blocking email attachments commonly associated with malware
- Blocking email attachments that cannot be scanned by antivirus software
- Implementing email filtering at the mail gateway and blocking suspicious IP addresses at the firewall
- Using multifactor authentication on all remote access systems
- Ensuring that all server and endpoint software is maintained at a current level, including all relevant security software.

Source: **BlackBerry Research/KPMG**

DHS shares data on top threats to federal agencies

Cybersecurity and Infrastructure Security Agency (CISA) analysts have compiled the top detection signatures through May 2020.

The signatures were detected by the national intrusion detection system (IDS), known as EINSTEIN, an automated process for collecting, correlating, analyzing and sharing computer security information across federal civilian departments and agencies. Threats include:

- **NetSupport Manager Remote Access Tool (RAT)**. This is a legitimate program that, once installed on a victim's machine, allows remote administrative control. In a malicious context, it can be used to steal information.
- **Kovter**. Kovter is a fileless Trojan with several variants that started as ransomware. Threat actors have also used Kovter to perform click-fraud operations to infect

targets and send stolen information from target machines to command and control servers. Kovter's evolving features have allowed this malware to rank among the Center for Internet Security's most prolific malware year after year.

- **XMRig**. This malware is a type of cryptocurrency miner that uses the resources of an infected machine to mine Monero. XMRig can cause a victim's computer to perform poorly by using additional system resources that would otherwise not be active.

Impact

RATs, fileless malware and miners pose serious threats to any enterprise. Given that EINSTEIN has seen these types of attacks more often than others provides areas of focus for security organizations.

All three attack types can affect the confidentiality and availability of data. In addition, cryptominers have the ability to install backdoors and should be viewed as more than uninvited users of resources. Once access is established to the affected machine, the ability to install other malware, exfiltrate sensitive data and perform espionage is an easy exercise.

XMRig, which can be used on both Windows and Linux machines, is open source and used to mine the Monero cryptocurrency. In 2017, threat actors began modifying the code to create malicious versions of XMRig.

DXC perspective

The intrusions detected by EINSTEIN should help as a guideline on how to allocate security resources. Not all environments will match the infrastructure of government agencies; therefore, security controls will vary by organization.

Sources:
Department of Homeland Security
CISA

Vulnerability Updates

SMBGhost combined with SMBleed poses preauthentication RCE threat

Discovered during an SMBGhost investigation by Zecops research team, SMBleed malware allows the leak of kernel memory remotely. Combined with SMBGhost, SMBleed allows attackers to achieve preauthentication remote code execution (RCE) on unpatched Windows 10 systems.

Impact

Because this vulnerability could be chained with the SMBGhost (CVE-2020-0796) to achieve preauthentication remote code execution, a successful exploit will provide threat actors with high privileged access and will allow lateral movement to connected machines.

DXC perspective

SMBGhost and SMBleed vulnerabilities have received a Common Vulnerability Scoring System (CVSS) 10 severity score, and organizations are advised to patch immediately. This is no longer a proof-of-concept attack. Both vulnerabilities have been observed in the wild actively exploiting affected machines. Microsoft has issued patches and mitigation workarounds if patching causes conflicts.

Sources:
Microsoft CVE-2020-0796
Microsoft CVE-2020-1206
Mitre

F5 BIG-IP vulnerability disclosed

A Positive Technologies researcher disclosed details on a vulnerability on F5 BIG-IP appliances that leads to remote code execution threats.

The vulnerability, which resides within the Traffic Management User Interface (TMUI) configuration utility, can be exploited by unauthenticated attackers or authenticated users. Attackers must have network access to the configuration utility through the BIG-IP management port and/or self IPs. The BIG-IP system in appliance mode is also vulnerable.

F5 included a **list of products affected** on its website.

1M

The UK's National Cyber Security Centre (NCSC) has received reports of 1 million suspicious emails since April 2020, an average of 16,500 daily emails.

Impact

This vulnerability has received a CVSS 10 severity score and may result in complete system compromise. The vulnerability has been assigned the following Common Vulnerabilities and (CVE) IDs, depending on the vendor:

- CVE-2020-5902
- CVE-2020-5903 - BIG-IP TMUI XSS vulnerability CVE-2020-5903

Threat actors have already begun to exploit the CVE-2020-5902 flaw to obtain passwords, create web shells and infect systems with malware.

Analysts at Bad Packets report ongoing mass scanning for vulnerable F5 BIG-IP servers. If successful, attackers can execute arbitrary system commands, create or delete files, disable services, and/or execute arbitrary Java code.

DXC perspective

Given the impact a successful exploit can have on a vulnerable server, immediate patching and/or remediation should occur. F5 has responded with a list of patches per product line and detailed instructions on how to mitigate this attack if a patch is not available or is unfeasible.

Use this Advanced Shell (bash) script to search for intrusion attempts: journalctl /bin/logger | grep -F '..;'

Other news

- European bank suffers biggest PPS DDoS attack, new botnet suspected - **Akamai**
- Ransomware gang claims attack on LG Electronics - **Bleeping Computer**
- Criminals intercepted payment card details used at Claire's online store - **Sky News**
- Cyber criminals likely poised to attack, as Adobe ends support for Magento 1 - **SC Media**
- DXC Technology update on Xchanging ransomware attack - **DXC Technology**

The above-mentioned mitigations are available on the F5 product support website.

F5 also recommends upgrading to the latest releases of BIG-IP versions if using public cloud marketplaces (AWS, Azure, Google Cloud Platform and Alibaba) to deploy the BIG-IP Virtual Edition.

If it is not possible to upgrade, add a LocationMatch configuration element to httpd to eliminate the ability of unauthenticated attackers to exploit this vulnerability.

Sources:
F5
Positive Technologies

Incidents/breaches

Honda Motor Company halts manufacturing operations due to ransomware attack

Honda confirmed to the BBC that a ransomware attack had halted operations in multiple countries, causing factories to shut down temporarily and disrupting other processes.

The attack, blamed on the Snake/EKANS ransomware, shut down factories in Japan, Europe and the United States.

"Honda can confirm that a cyber-attack has taken place on the Honda network," the Japanese car-maker said in a statement to the BBC. "There is also an impact on production systems outside of Japan."

Impact

Employees were unable to access email and other company IT resources. Voice communications were not functional for customer service or Honda financial services.

Honda's production facilities were affected as well, since EKANS also targets industrial control systems (ICS). Past attacks have shown that ICS is the primary target of EKANS, but investigators determined that the malware also targeted both customer services and financial services.

While the initial attack vector has not been publicly disclosed, investigators suspect remote desktop protocol (RDP) access, one of the main entry points when it comes to targeted ransomware.

DXC perspective

Ransomware attacks are on the rise and will continue, given how lucrative they are. Financially motivated threat actors have no reason to stop attacks that have such a high success rate.

Most EKANS attacks have been targeted, as the name of the organization affected has been hard-coded into the malware. Of even more importance is the fact that EKANS is coded in the Go programming language. Malware coded with this language is done to target multiple operating systems. Both Windows and Linux machines can be affected by EKANS with minimal effort on the part of threat actors.

The malware's ability to target industrial control systems makes it both disruptive and dangerous. EKANS stops processes from running on an affected machine. Under the right circumstances, this could have catastrophic results if, for example, the cooling system of a nuclear reactor were to stop functioning.

Preparation and planning are key components to stopping ransomware attacks. It is highly recommended for all organizations to obtain a copy of the U.S. Secret Service's "Preparing for a Cyber Incident: A Guide to Ransomware." The document contains valuable information that can be useful in combatting all types of malware attacks.

Sources:
BBC News
Dragos
Malwarebytes

17-year-old charged in Twitter VIP breach

FBI, IRS, U.S. Secret Service and Florida law enforcement officers charged a 17-year-old hacker in Tampa, Florida, with hijacking high-profile Twitter accounts and tweeting out a bitcoin scam that earned him more than $100,000.

Among the hijacked accounts were those of President Barack Obama, former Vice President Joe Biden, SpaceX chief executive officer Elon Musk, rapper Kanye West and Microsoft cofounder Bill Gates, as well as corporate accounts of Apple, Tesla and Uber.

The takeovers lasted more than 2 hours, and Twitter took extreme measures to prevent other verified accounts from being compromised, such as disabling the ability for some users to send new tweets and locking some users out of their accounts. The New York Times reported in July that "the hacker accessed Twitter's internal Slack messaging system and gained control of special tools that could be used to take over any Twitter account."

The U.S. Department of Justice on July 31 charged three people in connection with the hack: a 17-year-old "mastermind" with a $3 million bitcoin account; Nima Fazeli (aka "Rolex"), 22, of Orlando, Florida; and Mason Sheppard (aka "Chaewon"), 19, in the United Kingdom.

Impact

The hijacked Twitter tweaks included requests for bitcoin donations to support "giving back to the community." According to federal agents, Sheppard used a personal driver's license to verify himself with the Binance and Coinbase cryptocurrency exchanges, and his accounts were found to have received some of the scammed bitcoins, which overall totaled 12.86 bitcoin, or $117,457.58 from unwitting Twitter users.

The attackers also accessed the private direct messages of 36 Twitter users, including one elected official.

Twitter said the breach was caused by human error and a spear phishing attack on Twitter employees. Twitter said its staff members were targeted over the telephone and asked to reveal account usernames and passwords.

Social media is a major form of communication, and hacktivists have already successfully taken over Twitter accounts, motivated by the disbursement of misinformation. The latest Twitter breach was financially motivated and is an example of how the account takeover of trusted and highly followed users can be used to deceive in a relatively short window of time.

DXC perspective

This incident highlights three areas all organizations should focus on to protect user accounts and company information:

- Restrictions on publishing employee contact information and data
- Security awareness training
- Principle of least privilege. Employees should be granted only the privileges needed to complete their tasks.

Sources:
U.S. Department of Justice
Tampa Bay Times

DXC contains ransomware attack on Xchanging subsidiary

DXC announced in July that certain systems of its subsidiary, Xchanging, experienced a ransomware attack. Xchanging is primarily an insurance managed services business that operates on a standalone basis.

Impact

With an investigation into the attack nearly complete, DXC confirmed containment of the incident in the immediate days following identification with minimal impact on Xchanging customers; no loss of DXC or Xchanging customer data; no impact on the wider Xchanging or DXC IT estates; and full restoration of Xchanging customer operations.

DXC teams worked with affected Xchanging customers to restore access to their operating environments as quickly as possible and shared Indicators of Compromise (IOCs) and other relevant technical information.

The forensic review and investigation has involved appropriate law enforcement and cyber defense authorities and independent cyber security firms including Mandiant/FireEye. There were no indications of previous infection, spread beyond initially impacted Xchanging systems, or continued infection by the threat actor. There is currently no evidence that Xchanging, DXC or customer data was compromised or lost.

DXC perspective

Along with ongoing systems monitoring, DXC is continuously investing in and enhancing its cyber detection and response capabilities to effectively manage risk and safeguard customers and its IT estates with the continued growth of malicious attacks.

Sources:
DXC Technology

Nation State and Geopolitical

Iran hackers password spray U.S. power grid

In response to the killing of Iranian general Qasem Soleimani, Iran had promised an increase of cyber attacks aimed at U.S. assets. Preliminary evidence provided by Dragos indicates password spraying attacks have been aimed at American electric utilities.

Dragos has been monitoring the activity closely and attributed the hacking activity to Iranian APT33, aka Magnallium, Refined Kitten. Dragos has identified a second group working with APT33 named Parisite. Both groups are also targeting U.S. oil and gas facilities to gain access. The combined campaigns have been in progress since 2019.

Impact

The current tools available to the Iranian hackers lack the capabilities to access the software used to control the physical equipment in the power grid. However, Rob Lee, threat intel analyst and founder and chief executive officer of Dragos, warns that targeted utilities should monitor for breach attempts and assume that some assets have been compromised.

Many power grids are interconnected both on a national and international level so generation facilities can redirect surplus energy to regions of need. Such interconnectivity can be leveraged by threat actors to propagate across platforms.

DXC perspective

The toolsets and capabilities of Iranian threat actors have been underestimated in the past and should be considered dangerous today. Access to systems can be sold to other threat actors such as those mentioned above that run the Tycoon ransomware attacks. Alternatively, Iranian threat actors may use the access to launch other malware such as Shamoon, the disk wiper malware, or Hexane, the Remote Access Trojan used for DNSpionage.

Dragos' findings are an important reminder to practice basic cyber hygiene, patch regularly and use the most recent operating systems available if possible. Industrial control systems can be difficult and costly to maintain but allowing such systems to run on outdated operating systems can have catastrophic results.

Source:
Dragos
InfraGard
Department of Homeland Security

Russian threat actor group APT29 targets COVID-19 vaccine research

National security agencies in Canada, the United States and the United Kingdom say that throughout 2020, the Russian-linked group APT29 has targeted various organizations involved in COVID-19 vaccine development.

APT29 (aka "the Dukes" or "Cozy Bear"), a cyber espionage group and part of the Russian intelligence services, is using custom malware known as WellMess and WellMail to target several organizations, including those involved with COVID-19 vaccine development, according to the UK National Cyber Security Centre, Canada's Communications Security Establishment (CSE) and the U.S. Department of Homeland Security.

To mount the attacks, APT29 is using exploits for known vulnerabilities to gain initial access to targets, according to the analysis, along with spear phishing to obtain authentication credentials to internet-accessible login pages for target organizations. The exploits in rotation include the recent Citrix code-execution bug (CVE-2019-19781); a publicized Pulse Secure VPN flaw (CVE-2019-11510); and issues in FortiGate (CVE-2018-13379) and Zimbra (CVE-2019-9670).

Impact

The group conducted basic vulnerability scanning against specific external IP addresses owned by targeted organizations. The group then deployed public exploits against the vulnerable services identified.

The attempted theft of vaccine-related data puts at risk the confidentiality, integrity and availability of such data, potentially causing delays in the development of a COVID-19 vaccine. Any delays in such development will result in loss of human life.

DXC perspective

Intellectual property theft via cyber espionage is the main objective of many threat actors including state-sponsored APTs. To protect company assets, organizations must stay vigilant in all areas of information and physical security.

Sources:
United Kingdom's National Cyber Security Centre (NCSC)

Learn more

Thank you for reading the Security Threat Intelligence Report. Learn more about security trends and insights from **DXC Labs | Security**.

DXC in Security

Recognized as a leader in security services, DXC Technology helps clients prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24x7 managed security services are backed by 3,000 experts and a global network of security operations centers.

DXC provides solutions tailored to our clients' diverse security needs, with areas of specialization in Cyber Defense, Digital Identity, Secured Infrastructure and Data Protection. Learn how DXC can help protect your enterprise in the midst of large-scale digital change. Visit **www.dxc.technology/security**.

Stay current on the latest threats at www.dxc.technology/threats.

▶ **Get the insights that matter.**
www.dxc.technology/optin

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to deploy our enterprise technology stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at **www.dxc.technology**.

August 2020