DXC.technology

April 2019

Threat Intelligence Report

About this report

The DXC Threat Intelligence Report provides a monthly roundup of key developments related to the cyber threat landscape.

Leveraging a mix of open source and proprietary information feeds, including DXC Technology's global network of Security Operations Centers and cyber intelligence services, this report delivers a succinct overview of major incidents, insights into key trends and awareness of strategic threats so that you can take action.

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

By the numbers

2.2B

Unique usernames and passwords leaked onto the dark web in Collections #1-#5

$41M

Estimated cost of the Norsk Hydro cyber attack

Key takeaways

- Magecart compromises third-party suppliers' ability to prevent card skimming and emerges as a major threat to all e-commerce sites.
- Ransomware adversaries focus on enterprise-scale targets to maximize returns.
- Automation helps adversaries compress the cyber kill chain, reducing time for cyber defense to detect and disrupt attacks.
- Mobile malware attacks increased throughout 2018, with incidents of mobile Trojan.Droppers doubling.

Headlines this quarter

- **Citrix suffers breach by Iranian advanced persistent threat (APT) group Iridium**. The FBI says attackers used password spraying and proprietary techniques to defeat two-factor authentication and steal 6 terabytes of sensitive documentation. At the time the breach was disclosed, Citrix said it was not known whether it had affected the integrity of any Citrix services or clients. Iridium has previously targeted oil and gas, technology and government sectors.
- **North Korean-sponsored adversaries likely behind Operation Sharpshooter.** A key server used by the Lazarus Group to conduct attacks was reportedly compromised and monitored by McAfee researchers and U.S. law enforcement officials. They found that the attackers targeted the intellectual property of scores of organizations and continue to target finance, government and critical infrastructure in Germany, Turkey, the United Kingdom and the United States.
- **LockerGoga ransomware takes Norsk Hydro offline.** The Norwegian aluminum producer's CFO Eivind Kallevik said the entire worldwide network went down, affecting production operations. French engineering enterprise Altran also was affected by a significant LockerGoga infection.
- **FIN7 cyber crime group active again, following law enforcement disruption in Q3.** The notorious point-of-sale compromise group's latest campaign involves previously unseen malware types delivered via phishing emails. One, dubbed SQLRat, leaves no forensic evidence on the host system.
- **773 million unique email addresses and 21.2 million plain text passwords leaked in Collection #1 data dump.** The dump was available on file-sharing site MEGA and various criminal forums. DXC assesses that the stolen data is likely to be used in password-spraying attacks.

Notable Magecart groups

Groups 1 and 2

Use extensive automation to breach and skim sites; have a wide target array and a complex, customized reshipping infrastructure for monetization.

Group 3

Focuses on high-volume targeting, often in Latin America; uses unique skimmer checkout web pages to capture payment information.

Group 4

Sophisticated group that blends into "normal" web traffic by mimicking ad providers, analytic modules or victim domains; has 3,000+ possible compromises.

Group 5

Targets third-party suppliers to compromise multiple websites; implicated in the 2017 Ticketmaster breach.

Group 6

Focuses on largest organizations to secure high volume of transactions; responsible for British Airways and Newegg breaches in 2018.

Group 11

Skimmer with added capabilities for credential or sensitive information theft; responsible for Vision Direct breach in December 2018.

Group 12

Targets third parties to inject card-skimming code into multiple sites; responsible for the Adverline breach in late 2018.

Trends and developments

Magecart evolves tactics and techniques to sustain card-skimming activities

Magecart persists as a principal threat to all organizations processing payment card details online. Magecart card-skimming operations have affected thousands of organizations since 2015.

Rather than the name for a homogeneous criminal group, Magecart is a descriptor for the modus operandi of web skimming for payment data. Numerous criminal groups have been identified under this umbrella term, seven of which were highlighted in a joint RiskIQ and Flashpoint report published in November 2018. Each group is distinguished by unique variations in infrastructure, skimming code and targeting activity.

Further details concerning the structure and evolving methodology of Magecart emerged this quarter. These include the use of third-party compromise, top-level-domain (TLD) squatting and GitHub manipulation.

Group 12 shifts tactics to leverage third-party compromise

In early 2019, Magecart Group 12 grew to prominence. It has affected 277 ticketing, touring and flight-booking services as well as self-hosted shopping cart websites from major cosmetic, healthcare and apparel brands.

Group 12 leverages third-party compromise to expand the propagation of skimmer code. In late 2018, this group injected malicious JavaScript into a library by Adverline, a French online advertising company. This caused e-commerce sites embedded with the Adverline library to load the malicious library, compromising numerous Adverline customers' payment processing pages without targeting the individual payment processing sites directly. Prior to this, the group had performed only direct compromises of target sites.

Group 12 uses a unique skimming toolkit with two scripts. The first checks integrity and cleans the browser debugger console to disrupt detection attempts. The second identifies the payment page or checkout functions and then skims, encodes and exfiltrates the payment data using HTTP POST requests to a remote server controlled by the group.

Magecart uses top-level-domain (TLD) squat in MyPillow attacks

Magecart uses varied tactics to conceal its skimmer code.

MyPillow, a pillow manufacturing company, suffered a sustained Magecart compromise in late 2018. The attack first injected code into the MyPillow webstore that called payment-skimming code from an external malicious domain with a "typosquatted" name, mypiltow.com.

In a further attack, Magecart exploited its access to the MyPillow webstore to redirect calls made to livechat.com to livechat.org, a domain controlled by Magecart as a top-level-domain (TLD) squat. Using this redirection, Magecart was able to inject payment-skimming code into the webstore each time the store included code from LiveChat, without leaving any significant evidence or footprint on the MyPillow servers.

Visibility of third-party integrations, technical attack surface and domain hygiene can reduce card-skimming risk

Tuposquatting (URL hijacking)

The practice of purchasing a misspelled or mistyped version of a domain name. Often used by malicious actors who set up fake sites that imitate the look and feel of a legitimate site, typosquatting deceives users into providing sensitive data or downloading malware.

Magecart uses typosquatting to insert domain names into code that at first glance looks legitimate.

Top-level-domain (TDL) squatting

Same strategy as above, but rather than misspelled domain names, attackers purchase an alternative top-level domain.

Such tactics highlight that even minor changes to a web application can lead to significant security breaches that are difficult for operations staff to identify and could go unnoticed for extended periods of time.

GitHub utilized in attacks on Amerisleep

In an evolution of the attack on MyPillow, Magecart further camouflaged its activities during attacks on Amerisleep, a U.S. mattress retailer

In this instance, Magecart altered the webstore to include code from a GitHub repository under its control that included payment skimming and data exfiltration code. Magecart had named the repository “amerisleep” to generate an air of legitimacy around it. However, use of an established service such as GitHub caused the page to be quickly removed. Magecart has since returned to using its own squatter domains.

Sources: RiskIQ, Trend Micro, Flashpoint, Symantec

DXC perspective

Defending in depth against the Magecart threat should be central to the security strategy of all organizations processing payment card details through online stores. DXC assesses with high confidence that Magecart activity levels will continue to rise through 2020.

Visibility is key. Magecart’s recent tendencies to leverage third-party compromise highlight the importance of mapping where and how integrations occur. The security of partner organizations directly affects the security of companies connected to them via supply chain attacks. Visibility should extend to typosquatted domains and other developer services using variants of a target organization's name. Current attack trends suggest these are being leveraged to conceal malicious activity.

Magecart’s progression of tactics also reinforces the importance of securing internet-facing applications and infrastructure, as common techniques typically require some form of initial infrastructure compromise. Effective security monitoring, patching, credential management and infrastructure hardening are all essential in disrupting the access required to conduct card-skimming activities.

As password-spraying attacks increase, so does the likelihood of credential-skimming activity. Magecart’s primary focus will remain on payment card theft, but it is likely that Magecart and other cyber criminals will also step up the use of skimming methodologies to steal credentials. Two-factor authentication and credential management policies should be implemented wherever possible.

Ransomware adversaries focus on ‘big game hunting’ to maximize revenues

Sophisticated ransomware campaigns are increasingly focused on enterprise-scale targets as adversaries seek to maximize return on investment. Low-volume, high-yield operations using Ryuk and GandCrab ransomware variants have been witnessed, according to CrowdStrike and FireEye research. Recent incidents of LockerGoga ransomware infections, notably of Norsk Hydro, also follow this trend.

Adversaries combine automation with manual techniques in the kill chain to compress attack time scales. They typically achieve initial compromise via automated spam campaigns containing malware payloads or account compromise tools. Adversaries then use administrative and commonly available penetration testing tools to move

laterally across networks, compromising domain controllers and other high-value hosts to maximize the scale of infection.

Ryuk

Ryuk, operated solely by Grim Spider, initially compromises networks through either the notorious banking trojan TrickBot or Emotet, a banking trojan most commonly used to drop further malware. Delivered by largely automated spam campaigns, the group achieves compromise at mass but then progresses through the kill chain only when it identifies a target of sufficient size. Ryuk has targeted the financial, healthcare, hospitality, legal and retail sectors in the United Kingdom and North America.

$3.8M

Paid to Ryuk Bitcoin wallets

GandCrab

GandCrab ransomware, offered as a service by cyber criminal group Pinchy Spider, has been lucrative since early 2018. Recently, Pinchy Spider's tactics have shifted focus toward big game hunting. The group achieves initial access via credential compromise and remote desktop protocol (RDP) exploitation. It then uses various commercial and administrative tools to move laterally in the network, gaining access to domain controllers that can trigger further infections. Pinchy Spider has been advertising for affiliates with experience in RDP and virtual network computing to join the group, reinforcing its shift toward larger enterprise environments.

Ryuk and GandCrab infections typically follow initial compromise using alternative malware types.

LockerGoga

The recent and severe LockerGoga infection across the Norsk Hydro network may also follow the "big game hunting" trend. LockerGoga appears to selectively target organizations, affecting a handful of major industrial and manufacturing companies this quarter. Like other big game hunters, LockerGoga requires deployment by an attacker that already possesses network access at an administrative level. It leverages Active Directory for deployment across the target enterprise. The full LockerGoga kill chain remains unclear, though FireEye research suggests that stolen credentials are used for initial access, followed by the use of common penetration testing tools.

Source: CrowdStrike, FireEye

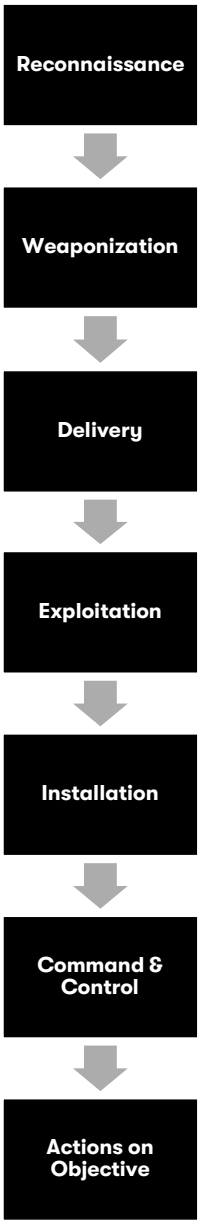
Mimikatz, PsExec, PowerShell Empire, LAN Search Pro, Sysinternals and Metasploit have all been used to by ransomware adversaries to navigate through networks.

DXC perspective

Focusing ransomware deployment on enterprise environments is nothing new. SamSam and BitPaymer, which extensively targeted healthcare providers, among other large organizations, set a precedent for big game hunting. However, recent trends reinforce the popularity of this approach and suggest a high level of attacker capability. LockerGoga, which has so far focused on the industrial sector, is likely to be adapted for targeting other specific industry verticals. DXC sees these trends continuing into 2020.

Countering the diverse methods used to gain initial access to target networks requires mature perimeter and account security. The malicious use of penetration testing and administration tools to navigate through the network highlights the need for organizations to use multilayered security to monitor and protect their internal networks as well as their borders. Next-generation endpoint protections, user and entity behavior analytics (UEBA) and security information and event management (SIEM) solutions are effective in building deep resilience.

Cyber kill chain compression



Source: Alert Logic

Automation helps adversaries compress the cyber kill chain

The traditional cyber kill chain is being compressed, according to Alert Logic's 2018 Critical Watch Report. The first five phases of the kill chain — reconnaissance, weaponization, delivery, exploitation and installation — now frequently occur in a single action. Automation and predefined weaponized packages make this compression possible.

The rise in cryptomining, currently the most common malware type in circulation, is central to this trend. With most networked devices potentially valuable targets for cryptominers, botnets scan the internet for vulnerabilities en masse, automating the delivery of exploit packages indiscriminately. Exploit packages typically automate further propagation of the malware, often using common protocols such as Secure Shell (SSH) or Server Message Block (SMB).

Automation of attacks continues to rise in more general terms, including:

- Pay and spray or automated credential stuffing attacks are being used to gain initial access for a diverse range of attacks.
- Adversaries are using artificial intelligence (AI), natural language processing and automation in the delivery of spear phishing campaigns. Previously, generating well-crafted emails for large groups of victims was resource- and time-intensive for attackers. But now, even where the kill chain phases remain distinct, automation is helping adversaries dramatically increase speed of action.
- The use of bots continues to increase for brute-forcing accounts, conducting denial-of-service attacks and extortion. This includes review bombing, in which bots damage a brand by overwhelming an organization with poor reviews. In February 2019, a major film review organization was forced to prevent user scoring of films due to continued review bombing attributed, in part, to Russian bots. Security analysts have also documented denial of inventory, the practice of bots placing items into shopping carts on e-commerce sites without checking out, thus making them unavailable for purchase by other users.

Source: Alert Logic

DXC perspective

The cyber kill chain remains relevant, and many adversary attacks are still aligned to traditional phases of activity.

However, automation is enabling significant kill chain compression for some attack types — notably in cryptomining — and some forms of ransomware. More generally, automation and AI are enabling adversaries to increase the speed of individual kill chain events.

With an accelerated kill chain, detection and disruption of attacks is more challenging. Security analysts have less time — or no time — to investigate and respond to threats.

Organizations will increasingly need to leverage automation and AI as an integrated part of their cyber defense. Machine learning modules in SIEM solutions and endpoint protections can assist in automated detection and disruption of a wide variety of threats in a considerably expedited time frame.

Security fundamentals play a central role in mitigating the risk of automated attacks. Visibility of your internet-facing attack surface, including internet of things (IoT), and vulnerability management are both essential.

The prominence of automated attack vectors means vulnerable web applications and internet-facing infrastructure will be targeted.

Mobile malware on the increase

As organizations embrace mobility, cyber adversaries increase their focus on exploiting it. Mobile malware incidents doubled in 2018, according to Kaspersky Lab, with almost 10 million users becoming affected by mobile malware variants. Mobile malware has been delivered via spam SMS and email, as well as DNS hijacking and malicious application attacks.

Trojan Droppers double

Trojan Dropper programs, which rose from 8.6 percent of malware observed in 2017 to more than 17 percent in 2018, bypass system protection and can deliver various malicious payloads, including banking trojans, adware and ransomware.

Trojan Droppers can be challenging to detect, as they evade signature-based protections by generating unique hashes for each instance.

Fivefold increase in cryptomining

The surge in cryptomining activity affects mobile as well as desktop and server platforms. Kaspersky's 2018 Mobile Malware Roundup Report noted a fivefold increase in cryptomining.

Drivers for the increase include the ease of mobile infection, as well as mobile devices' ubiquity and increase in power. Typically distributed via spam, mobile cryptominers can damage devices and degrade performance.

Social engineering via SMS delivers Asacub banking trojan

Banking trojans, delivered by SMS spam, continue to remain a common mobile attack vector. The Asacub trojan, prominent in 2018, was distributed using social engineering via SMS.

Once infected, the device sends SMS messages containing the trojan to the user's entire phonebook for further propagation. Increasingly, banking trojans exploit accessibility services to compromise banking applications on Android devices.

Source: Kaspersky Lab, Symantec

DXC perspective

Mobile device management and security present a constant challenge for organizations. Diversification in attacker techniques and delivery methods in exploiting mobile devices will likely continue.

Bring-your-own-device (BYOD) schemes serve to further complicate this environment. Diversification of mobile threats and their use in gaining initial access to corporate networks will be seen in FY20.

Mobile device security solutions can reduce the risks and offer better visibility into enterprise mobile exposure. Other methods of reducing risk include downloading applications only from official stores, blocking the installation of programs from unknown sources, and software patch management.

Keep current on the latest threats

Subscribe to the latest DXC threat intelligence updates. Visit www.dxc.technology/threats.

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 3,500+ experts and a global network of security operations centers.

DXC provides solutions tailored to our clients' diverse security needs, with areas of specialization in Intelligent Security Operations, Identity and Access Management, Data Protection and Privacy, Security Risk Management, and Infrastructure and Endpoint Security. Learn how DXC can help protect your enterprise during large-scale digital change. Visit www.dxc.technology/security.

About DXC Technology

As the world's leading independent, end-to-end IT services company, DXC Technology (NYSE: DXC) leads digital transformations for clients by modernizing and integrating their mainstream IT and by deploying digital solutions at scale to produce better business outcomes. The company's technology independence, global talent and extensive partner network enable 6,000 private and public-sector clients in 70 countries to thrive on change. DXC is a recognized leader in corporate responsibility. For more information, visit www.dxc.technology and explore thrive.dxc.technology, DXC's digital destination for changemakers and innovators.