

Security threat intelligence report

TeamTNT tool evades detection in cloud containers

7 key vulnerabilities in gateways and VPNs

Purple Fox malware gains worm capabilities

New APT34 backdoor emerges in phishing campaign

EtterSilent: A new malicious doc buildercontainers

June 2021



Table of contents

Threat updates

TeamTNT tool evades detection in cloud containers 3

New APT34 backdoor emerges in phishing campaign 4

Purple Fox malware gains worm capabilities 7

EtterSilent: A new malicious doc builder 8

Vulnerability updates

APT targets VPNs, gateways and collaboration services 8

Nation state and geopolitical

Federal agencies issue warning on APT29 group's activities 11

Message from Mark Hughes

Containers continue to be a key target for threat groups, and attackers are getting better at obscuring their attacks. Case in point: TeamTNT is targeting Docker and Kubernetes and using a new open-source tool to evade detection by common process information programs. This is a critical new threat to ever-expanding cloud environments. Also in this issue, federal authorities warn that attackers are exploiting seven high or critical vulnerabilities in widely used VPNs, gateways and collaboration services. Stay alert and up to date. These are times when good threat intelligence pays off.

Mark Hughes

Senior vice president
Offerings & Strategic Partners
DXC Technology

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:
May 11, 2021

46%

Percentage of malware that uses Transport Layer Security to conceal communications, up from 23% last year

Source: [Sophos](#)

2,400

Number of U.S.-based governments, healthcare facilities and schools hit by ransomware in 2020, according to Emsisoft

Source: [Krebs on Security](#)

533M

Number of Facebook users whose data was exposed in a recent breach

Source: [Forbes](#)

Threat updates

TeamTNT tool evades detection in cloud containers

Adversary group TeamTNT, which is known for exploiting unsecured Docker and Kubernetes daemons and deploying malicious container images, has been observed using new techniques to evade detection on systems it has compromised.

TeamTNT typically attacks Docker and Kubernetes environments to steal cloud credentials, open backdoors, mine cryptocurrency and deploy worms to scan for vulnerable hosts. TeamTNT is also linked to the first cryptomining worm to steal AWS credentials.

While the group's original goal was to compromise cloud infrastructure and launch XMRig cryptominers, current activity indicates a shift towards password harvesting and data exfiltration. The TeamTNT toolset can stop other miners on targeted systems, and now the group has added libprocesshider to elude detection.

Libprocesshider is an open source tool on [Github](#) from 2014 that can be used to hide malicious processes from process information programs such as 'ps' (a Unix command to list running processes) and 'lsof' (a Unix command to list open files).

The way it works is it hides processes under Linux using ld preloader. Preloading allows the system to start a custom shared library before other system libraries are loaded. If the custom shared library exports a function with the same signature of one located in the system libraries, the custom version will override it.

[AT&T Alien Labs](#) reports that TeamTNT delivers libprocesshider within a base64 encoded script hidden in the TeamTNT cryptominer binary or ircbot. The encoded script:

- Modifies the network DNS
- Sets persistence through system
- Drops and activates the new tool as a service
- Downloads the latest IRC bot configuration
- Clears evidence of activities to complicate defenses

Once libprocesshider is loaded, it hides the TeamTNT bot from process-viewer tools that use the file '/usr/bin/sbin' and removes traces by deleting bash history.

The existence of libprocesshider should be considered an attack indicator when hunting for malicious activity on a host.

Impact

TeamTNT's previous attacks show the group has the ability to find and infiltrate cloud environments. The group has also exhibited the ability to develop sophisticated malware at a rapid pace. This latest addition to its toolchest shows growing sophistication as the group explores how to keep mining and exfiltration processes from being detected.

Ryuk ransomware targets RDP

Recent intelligence has revealed that owners of the Ryuk ransomware are altering tactics. According to researchers, to gain initial entry, most Ryuk attacks this year target systems with remote desktop connections exposed on the internet. Ryuk is one of the oldest and most persistent ransomware threat organizations. Experts estimate the group has collected at least \$150 million in ransoms. One of its biggest hauls to date came from a victim that paid \$34 million to restore the organization's systems.

Source: [Bleepingcomputer](#)

DXC perspective

TeamTnT has multiple tools at its disposal and currently employs most of them during attacks. It is currently unknown what the group's plans are for harvested credentials. At the minimum, it is expected the group will continue to rack up access to more resources for its mining activities.

Proper configuration of cloud infrastructure and supporting tools will become more important as attacks of this nature become more prominent.

Source: [Alien Labs](#)

New APT34 backdoor emerges in phishing campaign

Iranian threat actor APT34 has been updating its arsenal of attack tools, and Check Point Research recently saw the group using a new backdoor the company nicknamed SideTwist.

As in earlier attacks, APT34 uses what Check Point Research calls "booby-trapped job opportunity documents" that are sent directly to targeted individuals.

In this case, the document containing the malware was a Microsoft Word document named Job-Details.doc (MD5: 6615c410b8d7411ed14946635947325e). The malware was first observed in January 2021 when a copy was uploaded to VirusTotal from a user in Lebanon, where many of APT34's targets reside (**Figure 1**).

The document lure is an employment offer for various positions at Ntiva IT consulting in Virginia, USA. The attack vector is unknown but assumed to be malspam.

Overview

The digital landscape is changing at a rate we could have never imagined. Today's digitally empowered and geographically distributed customers are radically connected, hyper informed, and always on. To survive and thrive in this customer-centric, data-driven economy, enterprises need to rethink the technology infrastructure on which they are building and deploying mission-critical cloud applications and move to a modern, distributed database platform, built for hybrid cloud. In doing so, enterprises can make data the centerpiece of their organization, build real-time value at epic scale, and innovate with ease and speed.

Ntiva Delivers

Ntiva delivers the always-on, active-everywhere distributed hybrid cloud database built on Apache Cassandra™. The foundation for full data autonomy and personalized, real-time applications at scale, Ntiva Enterprise makes it easy for enterprises to exploit hybrid and multi-cloud environments via a seamless data layer that eliminates the issues that typically come with deploying applications across multiple on-premises data centers and/or multiple public clouds.

We help many of the world's leading brands across industries transform their businesses by eliminating data silos and powering modern, mission-critical applications.

PERFORMANCE OF DUTIES

The Employee, hereby agrees that throughout his/her period of employment s/he shall devote his/her full attention and time, during working hours, to the performance of his/her duties and business affairs of the Employer, in addition to performing said duties faithfully and efficiently as directed by the CEO or Supervisor of the Employer. It is not the intention of the Employer to assign duties and responsibilities which are not typically within the scope and characteristics associated with this position, or of which may not be required of other employees of similar rank and position. However, the Employer reserves the right to increase and/or revise the Employee's role and responsibilities, whether through reorganization of his/her position or promotion. Any change in the Employee's pay scale, due to the change of responsibilities and/or promotion, will be at the sole discretion of the Employer.

COMPENSATION & BENEFITS

In accordance with the following terms and conditions period of employment, compensation for his/her services will be as follows: Employee will receive monthly salary of \$6000 to \$10000 with one month evaluations and/or rate increases as deemed appropriate and amount to be determined by the Supervisor of the Employee.

AMENDMENT OF AGREEMENT

Job Title	Description	Requirement	Insert *
Accountant	Ntiva is looking to hire an Accountant in Saudi Arabia, Kuwait and United Arab Emirates.	<ol style="list-style-type: none"> BS in Accounting or Finance. Minimum 3 years of experience. Meticulous. 	
Admin&Operations Coordinator	Ntiva is looking for an Admin& Operations Coordinator with minimum 1 year of experience.	<ol style="list-style-type: none"> Maintain delivery schedules and follow up on payments. Follow up and update the sales and finance department with due payment status. Handle the Service Level Agreements with the clients to ensure on-time renewal. Generate reports to management, upon request. Maintain inventory of parts and scanners. General office duties. 	
Account Manager	Ntiva is looking for an Account Manager in its Move division	<ol style="list-style-type: none"> Minimum two years of sales experience in a business-to-business, large/strategic customer segment. A record of achievement in the Account Manager position. Sells the firm's complete offering of products and services. Leads all aspects of the sales process, calling upon others to assist in solution development and proposal delivery, as needed, or as directed by management. 	
IT Manager	Ntiva is looking to hire a IT Manager in Saudi Arabia, Kuwait and United Arab Emirates.	<ol style="list-style-type: none"> Skills: good database and programming and network security skills. Background: Computer science / Computer engineer. Experience: 2-4 years of experience. Languages: English and Arabic are musts. French is a plus. Location: Saudi Arabia, Kuwait and United Arab Emirates. Package deal: Depending on profile. manage and to handle the business design and technical processes. Prepare/Send reports. Diagnose and repair Computers. Create relationships with mobile operators in Saudi Arabia, Kuwait and United Arab Emirates. Managing and maintaining the company's database and distribution platform. 	
Junior Accountant	Ntiva is looking to hire a Junior Accountant in Saudi Arabia, Kuwait and United Arab Emirates.	<ol style="list-style-type: none"> BS in Accounting or Finance. 0 to 1 year of experience. Meticulous. 	
Project Manager	Ntiva Reach is looking to hire a Project Manager in Saudi Arabia, Kuwait and United Arab Emirates.	<ol style="list-style-type: none"> BE in Computer/Telecommunication Engineering or BS in Computer Science. 2 Years of Experience in IT projects management or other. Fluent in Arabic, French, English. PMP Certificate is a plus. Organize / Good written and oral communication skills / Teamwork. Assist project management team in projects follow ups and documents preparation. 	

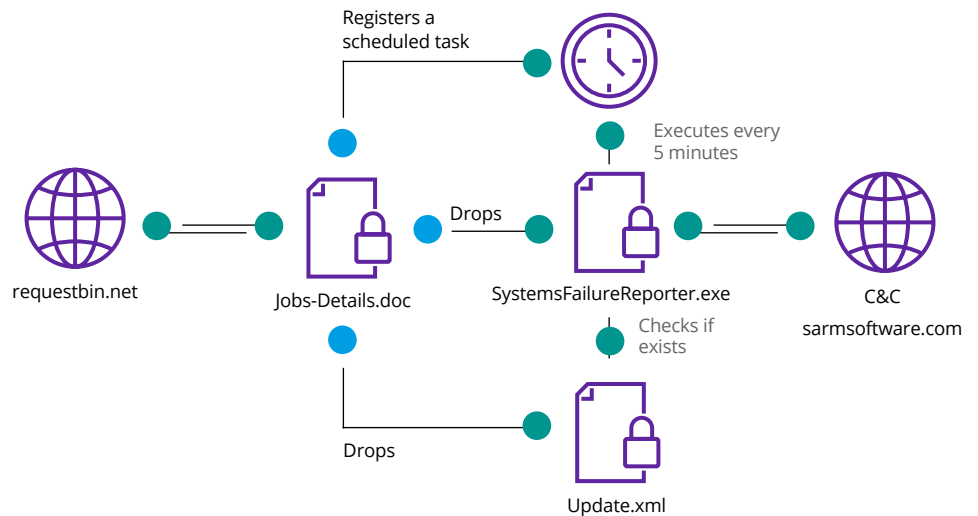
Figure 1. Example of malicious Word document with job offer

The Word doc contains malicious macros that, if enabled by the user, drop executables and schedule tasks:

Sodinokibi ransomware gang extorts Apple

One of Apple's primary suppliers has been the target of a recent ransomware attack from a Russian operator claiming to have stolen blueprints of the company's latest products. REvil, also known as Sodinokibi, claims to have infiltrated Quanta Computer, a key Apple supplier that primarily manufactures MacBooks. A user on the cyber crime forum XSS who is associated with REvil announced the group is on the brink of disclosing its "largest attack ever." REvil claimed it would disclose the Quanta compromise on the date of Apple's latest big reveal, noting that Quanta has stated it would not pay to recover stolen data. Quanta has acknowledged an attack without offering details. REvil is now attempting to extort Apple in its effort to profit from stolen data.

Source: [Bloomberg](#)



While SideTwist is new, like other APT34 attacks some macro functions are the same, Check Point Research reports:

- A check is made to see if a mouse is connected (an anti-sandboxing technique).
- The target device is fingerprinted and that information is sent to a C2 server.
- The embedded executable is dropped to disk with a "doc" extension (later to be renamed to ".exe").
- A Windows task is scheduled that will launch the executable every X-number of minutes.

Once the macros are executed, DNS requests are used to beacon back to the attacker data about the current stage of execution and victim identifiable information.

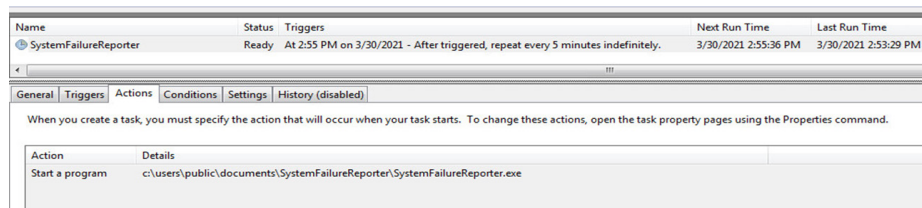
What's new with SideTwist is a variant of the second stage payload that creates a backdoor that is similar in functionality to other C-based backdoors such as DNSspionage, TONEDEAF and TONEDEAF2.0. SideTwist backdoor functions include file download, file upload and shell command execution.

But the second stage payload "does not have any persistence mechanism of its own," Check Point Research reports. Instead, that is accomplished in the first stage when the task schedule is registered. "The scheduled task named SystemFailureReporter will execute the 2nd stage payload every 5 minutes" (which represents a detection opportunity for hunters!).

Initial SolarWinds backdoor missed in August 2020

Both Microsoft and FireEye recently revealed in respective security blog posts a new backdoor found on high-value targets that were compromised as part of the SolarWinds attacks. Referred to as “Sunshuttle” by FireEye and “GoldMax” by Microsoft, the backdoor was named “Lexicon.exe.” A malicious file matching the MD5 and SHA-1 hashes was originally uploaded to VirusTotal in August 2020 by a U.S.-based entity. An analysis of the malicious file and other submissions by the same VirusTotal user suggests the account that initially flagged the backdoor belongs to IT personnel at the National Telecommunications and Information Administration (NTIA), a division of the U.S. Commerce Department that handles telecommunications and Internet policy. It would be four months before the news of SolarWinds and related breaches would be revealed to the world in early December 2020.

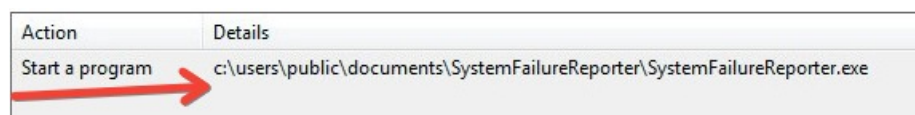
Source: [Security Boulevard](#)



Name	Status	Triggers	Next Run Time	Last Run Time
SystemFailureReporter	Ready	At 2:55 PM on 3/30/2021 - After triggered, repeat every 5 minutes indefinitely.	3/30/2021 2:55:36 PM	3/30/2021 2:53:29 PM

Action	Details
Start a program	c:\users\public\documents\SystemFailureReporter\SystemFailureReporter.exe

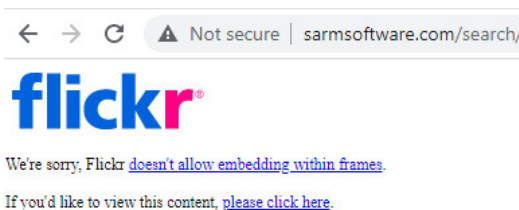
The backdoor relies heavily on this persistence mechanism. Each time the backdoor is launched, it executes a single command provided from the C2 server and then immediately shuts down and awaits relaunch by task scheduler. Note the scheduled task file location:



Action	Details
Start a program	c:\users\public\documents\SystemFailureReporter\SystemFailureReporter.exe

The malware communicates with C2 server sarmsoftware[.]com. Coms are HTTP based on port 443 with port 80 as fallback. The backdoor contacts the C2 server in the following URL using a GET request: sarmsoftware[.]com/search/{identifier}

The response to this request is hidden in the source code of the following Flickr lookalike page:



Impact

APT34 is in a rebuilding stage and this new backdoor indicates the group is developing new tools. The attack vector of malspam campaigns remains consistent with past activities. If successfully executed, SideTwist is capable of executing commands and exfiltrating data. APT34 demonstrates it is still a capable group with potential access to its own development resources.

DXC perspective

APT34 has a history of developing exploits for publicly known vulnerabilities. The group typically targets organizations in the Middle East. It is expected APT34 will continue to update its malware, including the incorporation of DGA for C2 to avoid detection.

It is uncertain at this time if APT34 will expand its targets outside of the Middle East region.

Sources: [Checkpoint](#), Malpedia, Any.run

Cyber criminals leverage HTTPS TLS to hide malware

A recent intelligence report from Sophos revealed just how widely Transport Layer Security (TLS) is used by cyber criminals to hide malicious activity. From January through March 2021, TLS was used to conceal communications of 45 percent of the malware Sophos analysts observed circulating on the Internet. That's double the rate — 23 percent — seen in early 2020. This surge in TLS abuse has driven the security community to shift its focus back to the firewall. TLS allows yet another mechanism for the attackers to obfuscate their malware as it is being moved into position and distributed. Once within networks TLS allows them to cloak any data as it is exfiltrated. While most organizations seek digital agility above all else, the need for a robust firewall to examine data streaming in and out has never been greater.

Source: [Sophos](#)

Purple Fox malware gains worm capabilities

The malware Purple Fox, which has traditionally been distributed using exploit kits and phishing emails, has been updated to include a worm that can be used to crawl the internet looking for Windows-based boxes to climb inside.

Purple Fox has rootkit and backdoor functions and is commonly used to download other malware. According to Guardicore Labs security researchers Amit Serper and Ophir Harpaz, usage began to increase significantly in May 2020, reaching a total of 90,000 attacks.

With the new worm capability, Purple Fox finds vulnerable Windows systems and then launches an SMB brute force attack to gain access. Guardicore says the tool has been used to compromise almost 2,000 servers, most of them running IIS version 7.5, and Microsoft FTP, Microsoft RPC, Microsoft Server SQL Server 2008 R2, Microsoft HTTPAPI httpd 2.0, and Microsoft Terminal Service.

Once inside, Purple Fox is said to load an open-source rootkit (<https://github.com/JKornev/hidden/>) that is used to hide dropped files and folders. When the machine is rebooted, the payload is renamed to match the local DLL and ensure that it is launched on restart. Each compromised machine then starts the process anew, looking for other machines to infect.

Impact

The main goal of Purple Fox is to drop other malware. The latest functionality allows the malware to worm across the network. The attack vector has also expanded to compromise a machine via a vulnerable exposed service such as SMB. Purple Fox has also added persistence methods as well.

DXC perspective

Purple Fox has been in existence since 2018 and continues to evolve today. The malware authors retool Purple Fox as security controls mature. Secure email gateways and system hardening procedures are effective steps to preventing Purple Fox from compromising a network.

Sources: [Minerva Labs](#), Malpedia

Task force seeks to disrupt ransomware payments

Amazon, Cisco, FireEye, McAfee and Microsoft have joined dozens of other firms to work with the U.S. Department of Justice, Europol and the U.K. National Crime Agency to create an international coalition to combat ransomware criminals. The Ransomware Task Force seeks to create a global network of investigation hubs to make finding, frustrating and apprehending ransomware crooks a priority within the global community. The Wall Street Journal recently broke the story that the DOJ was forming a task force to deal with the “root causes” of ransomware. An internal DOJ memo called for the development of “a strategy that targets the entire criminal ecosystem around ransomware, including prosecutions, disruptions of ongoing attacks and curbs on services that support the attacks, such as online forums that advertise the sale of ransomware or hosting services that facilitate ransomware campaigns.” Security firm Emsisoft reports that almost 2,400 U.S.-based governments, healthcare facilities and schools were victims of ransomware in 2020.

Source: [Wall Street Journal](#)

EtterSilent: A new malicious doc builder

On April 6, 2021, Intel471 reported a new malicious document builder called EtterSilent. This tool is regularly updated to avoid detection and is used by several threat actors, including the operators behind Trickbot, IcedID, QBot, Ursnif (aka Gozi) and Bazar.

EtterSilent is said to be able to bypass detection by Windows AMSI, Windows Defender and email services such as Gmail.

There are two versions of EtterSilent: one that targets Microsoft Office CVE-2017-8570 and another that relies on macros, with the latter being the more popular choice due to the ability to target a wider range of victims.

The Microsoft Office documents currently use a DocuSign theme. If the Excel 4.0 macros are enabled by the user, a payload download takes place. This has led to very widespread use of the tool. EtterSilent has the ability to weaponize Microsoft Office 2007 to 2019.

Impact

The TTPs of EtterSilent are difficult to track as the malware is sold on dark web forums. Most notably, the malware has switched from relying on Excel 4.0 macros to using DocuSign documents as a lure, which has met with great success.

DXC perspective

EtterSilent is being used by numerous groups to deliver a variety of malware including Trickbot and BazarLoader. Additionally, the malware infrastructure is known to be hosted on different bulletproof hosting services. Expect EtterSilent campaigns to continue and expand in volume.

Source: [Intel471](#)

Vulnerability updates

APT targets VPNs, gateways and collaboration services

On April 15, 2021, the U.S. National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) jointly released a Cybersecurity Advisory on the exploitation of known vulnerabilities by the Russian Foreign Intelligence Service (SVR), possibly as early as April 2019.

The SVR has exploited — and continues to successfully exploit — software vulnerabilities to gain footholds in victim devices and networks, leveraging: CVE-2018-13379 Fortinet, CVE-2019-9670 Zimbra, CVE-2019-11510 Pulse Secure, CVE-2019-19781 Citrix, CVE-2020-4006 VMware.

On April 20, 2021, CISA reported threat actor exploitation of additional known vulnerabilities in Pulse Connect Secure (VPN) server.

CVE Identifier	Description	CVSS Version 3.x Score — Rating
CVE-2018-13379	Fortinet FortiGate VPN	9.8 — Critical
CVE-2019-9670	Synacor Zimbra Collaboration Suite	9.8 — Critical
CVE-2019-11510	Pulse Secure Pulse Connect Secure VPN	10 — Critical
CVE-2020-8243	Pulse Secure Pulse Connect Secure VPN	7.2 — High
CVE-2020-8260	Pulse Secure Pulse Connect Secure VPN	7.2 — High
CVE-2019-19781	Citrix Application Delivery Controller and Gateway	9.8 — Critical
CVE-2020-4006	VMware Workspace ONE Access	9.1 — Critical

CISA is aware of compromises affecting U.S. government agencies, critical infrastructure entities and other private sector organizations by a cyber threat actor — or actors — beginning in June 2020 or earlier related to vulnerabilities in certain Ivanti Pulse Connect Secure products.

To gain initial access, the threat actor is leveraging multiple vulnerabilities, including CVE-2019-11510, CVE-2020-8260 and CVE-2020-8243.

CVE Identifier — Vendor Product	Advisory Link
CVE-2018-13379 Fortinet FortiGate VPN	https://www.fortiguard.com/psirt/FG-IR-18-384
CVE-2019-9670 Synacor Zimbra Collaboration Suite	https://bugzilla.zimbra.com/show_bug.cgi?id=109129
CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101
CVE-2020-8243 Pulse Secure Pulse Connect Secure VPN	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44588
CVE-2019-19781 Citrix Application Delivery Controller and Gateway	https://support.citrix.com/article/CTX267027
CVE-2020-4006 VMware Workspace ONE Access	https://www.vmware.com/security/advisories/VMSA-2020-0027.html
CVE-2020-8260 Pulse Secure Pulse Connect Secure VPN	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44588

DXC perspective

Advanced persistent threat (APT) groups are increasingly probing for and leveraging known vulnerabilities in VPNs, gateway products and collaboration service applications.

The ever-decreasing time to public release of exploit code further reduces the time for organizations to patch said products.

DXC CTI recommends:

- Patching to address known product vulnerabilities
- Increased patch cadence for VPNs, gateway products and collaboration service applications directly exposed to the Internet

Sources: [NSA](#), [DoD](#), [CISA](#)

Nation state and geopolitical

Federal agencies issue warning on APT29 group's activities

The SolarWinds campaign highlighted the group's sophisticated toolset, ingenuity and ability to remain undetected. Supply chain attacks will continue to evolve and most likely increase in occurrence given the success of SolarWinds.

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) recently released a Trends and Best Practices for Network Defenders alert (AA21-116A) concerning the Russian Foreign Intelligence Service (SVR) Cyber Operations.

The SVR, also known as Advanced Persistent Threat 29 (APT29), the Dukes, CozyBear and Yttrium, is Russia's external intelligence agency. The purpose of the advisory is to expose the SVR's ongoing exploitation of five publicly known vulnerabilities.

This advisory was released alongside the U.S. Government's formal attribution of the SolarWinds supply chain compromise and related cyber espionage campaign.

The advisory highlights additional tactics, techniques and procedures being used by SVR. The agencies urge users to mitigate against the following publicly known vulnerabilities:

- CVE-2018-13379 Fortinet FortiGate VPN
- CVE-2019-9670 Synacor Zimbra Collaboration Suite
- CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN
- CVE-2019-19781 Citrix Application Delivery Controller and Gateway
- CVE-2020-4006 VMware Workspace ONE Access

DXC perspective

APT29 has been in existence since at least 2008. The group is well known for its cyber-espionage attacks targeting Europe and NATO member countries and private sector organizations.

The SolarWinds campaign highlighted the group's sophisticated toolset, ingenuity and ability to remain undetected. Supply chain attacks will continue to evolve and most likely increase in occurrence given the success of SolarWinds. It is expected other threat actors will pivot off of this method as well.

Source: [CISA](#)

DXC in security

Recognized as a leader in security services, DXC Technology helps customers 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 customers' 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 largescale digital change. Visit www.dxc.technology/security.

Learn more at
dxc.com/threats

Get the insights that matter.

dxc.com/optin

