Security threat intelligence report

BlackMatter ransomware identified as successor to DarkSide, REvil

Shlayer malvertising campaigns still using Flash update disguise

SOLAR SPIDER targets financial institutions in India and Middle East

MacOS and IOS bugs patched

New report: top 30 routinely exploited vulnerabilities

September 2021

Table of contents

Threat updates

Vulnerability updates

Nation state and geopolitical

Message from Mark Hughes

Cybercriminal groups are constantly innovating and staying ahead of the authorities. BlackMatter, a new ransomware affiliate group, has been identified as the successor to major groups DarkSide and REvil, targeting firms with greater than $100 million in revenues. Using the growing ransomware-as-a-service business model, BlackMatter claims it has incorporated the best features of available ransomware tools and tactics into its services. This development underscores the need for more focus on vulnerability management, backups and highly coordinated ransomware response plans.

Mark Hughes
President of Security
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.

Intelligence cutoff date:
August 18, 2021

38M

Records found open on the internet, including data from COVID-19 contact tracing platforms, vaccination sign-ups and job portals, through Microsoft Power Apps portal service

Source: Wired

17.2M

Volume of HTTP requests per second in a DDoS attack against a Cloudflare customer, described as three times larger than any previous publicly disclosed attack

Source: The Record

47M

Number of current, former and prospective T-Mobile customers impacted by a data breach, for sale on an underground forum for 6 bitcoins (approximately $270,000)

Source: Reuters

Threat updates

BlackMatter ransomware identified as successor to DarkSide, REvil

BlackMatter, a new ransomware affiliate program founded in July 2021, is said to be the successor to major cybercrime groups DarkSide and REvil, according to reports by Recorded Future.

Flashpoint also reported on the new group's activities that month after observing BlackMatter register an account on the Russian-language underground forums XSS and Exploit and deposit 4 bitcoins (approximately $150,000) into its escrow account. Large deposits on the forum indicate the seriousness of the threat actor. On July 21 BlackMatter posted on the forums that the group is actively seeking to purchase access to infected corporate networks in the United States, Canada, Australia and United Kingdom. BlackMatter is looking for larger corporate networks with revenues exceeding $100 million.

According to BlackMatter's news release, "The project has incorporated in itself the best features of DarkSide, REvil and LockBit. The infrastructure security system is also thoroughly worked out. The project uses a decentralized structure and is protected from local file inclusion (LFI), SQL injection (SQLi), cross-site scripting (XSS) and other vulnerabilities."

Impact

RaaS groups have been observed merging and reorganizing. Reasons for this activity are usually due to group restructuring, tooling and prior incarnations being labeled as terrorist organizations. This strategy also helps to upgrade malware tools to increase the attack service and increase their impact upon compromise.

DXC perspective

DXC Technology will continue to monitor for new details as additional information becomes available. A joint advisory released by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) provides a robust list of mitigations and recommendations to both reduce the risk of compromise and prevent ransomware attacks.

Sources

Recorded Future
Flashpoint

Shlayer malvertising campaigns still using Flash update disguise

Malvertising campaigns delivering Shlayer malware for macOS are still ongoing, despite the patching of a critical zero-day vulnerability (CVE-2021-30657). This vulnerability was abused for months to compromise victims by dodging built-in OS protections such as Gatekeeper and also bypassing File Quarantine and Application Notarization. Recent Shlayer campaigns continue to use fake Flash updates and social engineering tactics to trick victims into manually installing the macOS malware and compromising their systems.

Impact

What separates Shlayer malware from other malware is its ability to leverage shell scripts to download additional malware or adware onto the infected device. Shlayer can escalate privileges to root by asking the user for credentials. It also uses bash scripts to check the macOS version and download payloads, and it can disable Gatekeeper using the native spctl application.

DXC perspective

Mac devices and macOS have historically been viewed as more secure because most hackers have focused on PCs and Windows vulnerabilities. This malware is a major potential threat to the education, research and publishing sectors, but includes all enterprises that use Apple products in their environment. DXC advises IT organizations to immediately identify Mac users, including BYOD computers accessing networks, and apply Apple's emergency patch for CVE-2021-30657. Cyber awareness training should include anti-phishing education that warns against the long-running Flash update lure.

Source

Crowdstrike

SOLAR SPIDER JsOutProx campaigns target financial institutions across India and Middle East

Multiple SOLAR SPIDER campaigns are distributing the JsOutProx remote access tool (RAT), targeting financial institutions in India, the Middle East and North Africa with financial-themed phishing emails spoofing the organizations to deliver the RAT malware. One attack in India employed an email sent from a compromised address corresponding to a recruiting firm.

Intelligence indicates Solar Spider's tactics, techniques and procedures include financial-themed phishing emails, 7ZIP archives and DDNS C2 domains that remain largely unchanged with the exception of using malicious javascript to distribute the malware.

Impact

Many of the campaigns observed redirect users to a URL containing the malicious javascript and associated malware. Malware delivered by infected JavaScript files do not require user interaction, increasing the success rate of campaigns.

DXC perspective

This adversary frequently targets these regions and will continue to pose a high risk to enterprises. However, SOLAR SPIDER does not limit targets to these specific regions. DXC intelligence analysts have observed campaigns targeting other regions as well.

Source

Malpedia

Vulnerability updates

MacOS and IOS bugs patched for CVE-2021-30807

Apple released an emergency zero-day patch addressing CVE-2021-30807. The bug is a memory corruption flaw that may allow an application to execute arbitrary code with kernel privileges. Apple claims that an exploit may be available in the wild. The flaws were fixed in the macOS Big Sur 11.5.1 update and a separate patch bundle that brings iOS and iPad devices up to version 14.7.1. The newest patch came less than a week after Apple shipped iOS 14.7 with fixes for a wide range of security issues.

- **Apple security Advisories:**
    - MacOS - https://support.apple.com/en-us/HT212622
    - iOS - https://support.apple.com/en-us/HT212623
- **PoC Exploit:** https://saaramar.github.io/IOMobileFrameBuffer_LPE_POC/

DXC perspective

The update file is large, about 2GB, but it is recommended that systems be upgraded immediately. Refer to the Apple advisory for resolution methods and workarounds.

Source

Apple Service Advisory

New report: Top 30 routinely exploited vulnerabilities

The top 30 vulnerabilities routinely exploited by malicious cyber actors in 2020 and thus far in 2021 were released by U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre, the United Kingdom's National Cyber Security Centre and the U.S. Federal Bureau of Investigation.

Most common CVEs exploited in 2021:

- Microsoft Exchange: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065
- Pulse Secure: CVE-2021-22893, CVE-2021-22894, CVE-2021-22899, and CVE-2021-22900
- Accellion: CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104
- VMware: CVE-2021-21985
- Fortinet: CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591

Top routinely exploited CVEs in 2020

Vendor	CVE	Type
Citrix	CVE-2019-19781	arbitrary code execution
Pulse	CVE 2019-11510	arbitrary file reading
Fortinet	CVE 2018-13379	path traversal
F5- Big IP	CVE 2020-5902	remote code execution (RCE)
MobileIron	CVE 2020-15505	RCE
Microsoft	CVE-2017-11882	RCE
Atlassian	CVE-2019-11580	RCE
Drupal	CVE-2018-7600	RCE
Telerik	CVE 2019-18935	RCE
Microsoft	CVE-2019-0604	RCE
Microsoft	CVE-2020-0787	elevation of privilege
Netlogon	CVE-2020-1472	elevation of privilege

DXC perspective

Knowing your infrastructure and routine hygiene can prevent intrusions related to these vulnerabilies. According to CISA, "Cyber actors continue to exploit publicly known — and often dated — software vulnerabilities against broad target sets, including public and private sector organizations worldwide. However, entities worldwide can mitigate the vulnerabilities listed in this report by applying the available patches to their systems and implementing a centralized patch management system." Refer to the CISA advisory for resolution methods and workarounds.

Source

CISA

New PetitPotam NTLM relay attack lets hackers take over Windows domains

PetitPotam, a newly uncovered Windows security flaw, marks the third major Windows security issue disclosed over the past month after the PrintNightmare and SeriousSAM (aka HiveNightmare) vulnerabilities. The flaw can be exploited to coerce remote Windows servers, including domain controllers, to authenticate with a malicious destination, thereby allowing an adversary to stage an NTLM relay attack and completely take over a Windows domain.

- Microsoft recommends that customers disable NTLM authentication on the domain controller. In the event NTLM cannot be turned off for compatibility reasons, additional mitigation steps can be found in its security advisory.
- A proof-of-concept exploit, dubbed PetitPotam, was shared on GitHub.

DXC perspective

DXC recommends users and administrators review KB5005413 and apply the necessary mitigations.

Source

Microsoft

Nation state and geopolitical

Lessons learned from the Tokyo Olympics 2021

Not surprisingly, the Tokyo Summer Olympics was a prime target for nation-state actors. The Federal Bureau of Investigation released a warning that adversaries were highly likely to be targeting all organizations and entities associated with the Tokyo 2020 Summer Olympics. Conflicting reports indicate there may have been a data breach of user IDs and passwords for the Tokyo Olympic ticket portal and the data may have been posted to a leak website.

Impact

Authorities believe RedLine malware and other information stealers may have been involved in the attack. RedLine is an information stealer that has the capability of executing commands, downloading files and periodically sending information about the infected system to threat actors.

DXC perspective

DXC will continue to investigate the vulnerabilities exploited in this attack to determine relevance to other organizations. Please refer to the FBI advisory for best practices.

Source

FBI

Other news

1 million compromised payment cards available for free

Wiper malware halts Iranian trains

Millions of senior citizens’ personal data exposed by misconfiguration

Accenture confirms LockBit ransomware attack

Hackers selling Lithuanian Ministry of Foreign Affairs emails (including attachments) on data-trading forum

Olympics broadcaster announces computer password on live TV

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 Risk Management. Learn how DXC can help protect your enterprise in the midst of large-scale digital change. Visit dxc.com/security.

Stay current on the latest threats
dxc.com/threats

Get the insights that matter.
dxc.com/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. The world's largest companies and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. Learn more about how we deliver excellence for our customers and colleagues at **dxc.com**.