Researchers compile list of vulnerabilities abused by ransomware gangs

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)**

September 18, 2021 10:00 AM **0**

Security researchers are compiling an easy-to-follow list of vulnerabilities ransomware gangs and their affiliates are using as initial access to breach victims' networks.

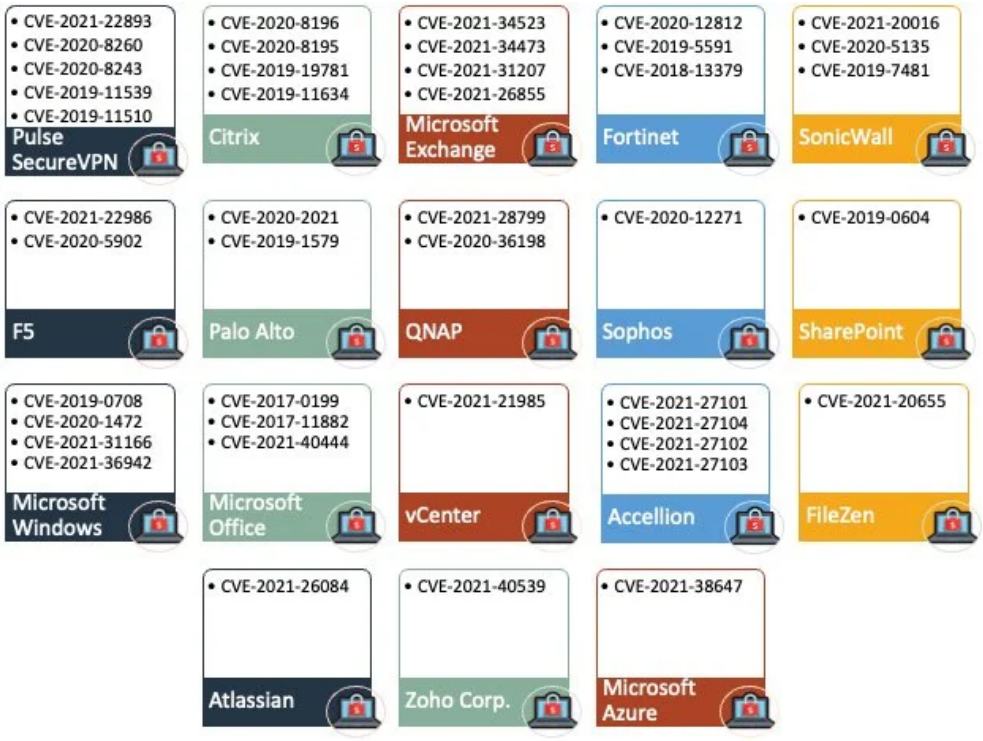
All this started with a call to action made by Allan Liska (https://twitter.com/uuallan/status/1436852174621925376), a member of Recorded Future's CSIRT (computer security incident response team), on

Twitter over the weekend.

Since then, with the help of several other contributors that joined his efforts, the list quickly grew to include security flaws found in products from over a dozen different software and hardware vendors.

While these bugs have been or still are exploited by one ransomware group or another in past and ongoing attacks, the list has also been expanded to include actively exploited flaws, as security researcher Pancak3 explained (https://twitter.com/pancak3llullz/status/1438904720266076168).

The list comes in the form of a diagram providing defenders with a starting point for shielding their network infrastructure from incoming ransomware attacks.



Vulnerabilities exploited by ransomware gangs (Allan Liska / Pancake (https://twitter.com/uuallan/status/1438899102448820224))

Vulnerabilities targeted by ransomware groups in 2021

This year alone, ransomware groups and affiliates have added multiple exploits to their arsenal, targeting actively exploited vulnerabilities.

For instance, this week, an undisclosed number of ransomware-as-a-service affiliates have started using RCE exploits (https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-mshtml-bug-now-exploited-by-ransomware-gangs/) targeting the recently patched Windows MSHTML vulnerability (CVE-2021-40444).

In early September, Conti ransomware also began targeting Microsoft Exchange servers (https://www.bleepingcomputer.com/news/security/conti-ransomware-now-hacking-exchange-servers-with-proxyshell-exploits/), breaching enterprise networks using ProxyShell vulnerability exploits (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207).

In August, LockFile started leveraging the PetitPotam NTLM relay attack method (https://www.bleepingcomputer.com/news/security/lockfile-ransomware-uses-petitpotam-attack-to-hijack-windows-domains/) (CVE-2021-36942) to take over the Windows domain worldwide, Magniber jumped on the PrintNightmare exploitation train (https://www.bleepingcomputer.com/news/security/ransomware-gang-uses-printnightmare-to-breach-windows-servers/) (CVE-2021-34527), and eChoraix was spotted targeting both QNAP and Synology NAS devices (https://www.bleepingcomputer.com/news/security/echoraix-ransomware-now-targets-both-qnap-and-synology-nas-devices/) (CVE-2021-28799).

HelloKitty ransomware targeted vulnerable SonicWall devices (CVE-2019-7481) in July, while REvil breached Kaseya's network (CVE-2021-30116, CVE-2021-30119, and CVE-2021-30120) and hit roughly 60 MSPs using on-premise VSA servers and 1,500 downstream business customers [1 (https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-1-000-plus-companies-in-msp-supply-chain-attack/), 2 (https://www.bleepingcomputer.com/news/security/kaseya-was-fixing-zero-day-just-as-revil-ransomware-sprung-their-attack/), 3 (https://www.bleepingcomputer.com/news/security/kaseya-patches-vsa-vulnerabilities-used-in-revil-ransomware-attack/)].

FiveHands ransomware was busy exploiting the CVE-2021-20016 SonicWall vulnerability (https://www.bleepingcomputer.com/news/security/new-ransomware-group-uses-sonicwall-zero-day-to-breach-networks/) before being patched in late February 2021 (https://www.bleepingcomputer.com/news/security/sonicwall-firewall-maker-hacked-using-zero-day-in-its-vpn-device/), as Mandiant reported in June.

QNAP also warned of AgeLocker ransomware attacks (https://www.bleepingcomputer.com/news/security/qnap-warns-of-agelocker-ransomware-attacks-on-nas-devices/) on NAS devices using an undisclosed flaw in outdated firmware in April, just as a massive Qlocker ransomware campaign targeted QNAP devices unpatched against a hard-coded credentials vulnerability (https://www.bleepingcomputer.com/news/security/qnap-removes-backdoor-account-in-nas-backup-disaster-recovery-app/) (CVE-2021-28799).

The same month, Cring ransomware started encrypting unpatched Fortinet VPN devices (CVE-2018-13379) on industrial sector companies' networks after a joint FBI and CISA warning (https://www.bleepingcomputer.com/news/security/fbi-and-cisa-warn-of-state-hackers-attacking-fortinet-fortios-servers/) that threat actors were scanning for vulnerable Fortinet appliances.

In March, Microsoft Exchange servers worldwide were hit by Black Kingdom [1 (https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-now-targeted-by-black-kingdom-ransomware/), 2 (https://www.bleepingcomputer.com/news/security/microsoft-black-kingdom-ransomware-group-hacked-15k-exchange-servers/)] and DearCry (https://www.bleepingcomputer.com/news/security/dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/) ransomware as part of a massive wave of attacks directed at systems unpatched against ProxyLogon vulnerabilities (https://www.bleepingcomputer.com/tag/proxylogon/) (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065).

Last but not least, Clop ransomware attacks (https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/) against Accellion servers (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104) that took place between mid-December 2020 and continued in January 2021 drove up the average ransom price (https://www.bleepingcomputer.com/news/security/accellion-data-breaches-drive-up-average-ransom-price/) for the first three months of the year.

Fight against an escalating ransomware threat

Liska's and his contributors' exercise adds to an ongoing effort to fend off ransomware attacks that have plagued worldwide public and private sector organizations for years.

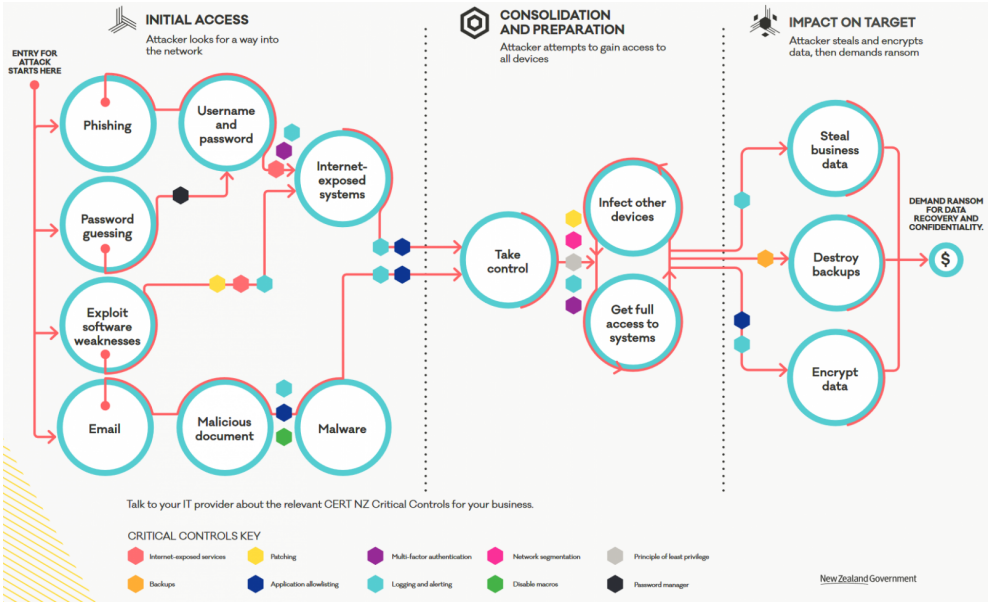
Last month, CISA was joined by Microsoft, Google Cloud, Amazon Web Services, AT&T, Crowdstrike, FireEye Mandiant, Lumen, Palo Alto Networks, and Verizon as part of the Joint Cyber Defense Collaborative (JCDC) partnership focused on defending critical infrastructure from ransomware (https://www.bleepingcomputer.com/news/security/cisa-teams-up-with-microsoft-google-amazon-to-fight-ransomware/) and other cyber threats.

The federal agency also released a new ransomware self-assessment security audit tool (https://www.bleepingcomputer.com/news/security/cisa-releases-new-ransomware-self-assessment-security-audit-tool/) in June designed to help at-risk organizations understand if they're equipped to defend against and recover from ransomware attacks targeting information technology (IT), operational technology (OT), or industrial control system (ICS) assets.

CISA provides a Ransomware Response Checklist (https://www.cisa.gov/stopransomware/ive-been-hit-ransomware) for organizations that have been hit by a ransomware attack, advice on how to protect against ransomware (https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware), and answers to frequently asked questions about ransomware (https://www.cisa.gov/stopransomware/ransomware-faqs).

The New Zealand Computer Emergency Response Team (CERT NZ) has also recently published a guide on ransomware protection for businesses (https://www.cert.govt.nz/business/guides/protecting-from-ransomware/).

CERT NZ's guide outlines ransomware attack pathways and illustrates what security controls can be set up to protect from or stop an attack.



CERT NZ ransomware attack guide