See what it's like to have a partner in the fight.

redcanary.com/blog/intel-insights-sept-2021/

Each month, the Intel team provides Red Canary customers with an analysis of trending, emerging, or otherwise important threats that we've encountered in confirmed threat detections, intelligence reporting, and elsewhere over the preceding month. We call this report our "Intelligence Insights" and plan to share a public version of it with the broader infosec community from here onward.

Highlights

Rose Flamingo dipped its pink talon into the top 10 confirmed threats we detected in August 2021. Meanwhile, TA551 continues to surge ahead of Cobalt Strike as the most prevalent threat from the last month—and year-to-date for that matter. We're also continuing to observe a trend of adversaries exploiting enterprise applications for initial access, primarily through vulnerabilities in WebLogic and Confluence over the last few weeks. Last but certainly not least, "Crypters" are gaining momentum among "as-a-Service" threats and lowering the barrier of entry for adversaries seeking to install remote access trojans (RAT).

The Red Canary Intelligence team offers insights into these threats—and a glimpse into the 10 most prevalent threats from August—in the latest edition of Intelligence Insights.

TOP THREATS IN AUGUST 2021

August rank	Threat name	Percent of customers affected
August rank : ➡ 1	Threat name: TA551	Percent of customers affected : 2.5%
August rank : ⬆ 2	Threat name: Cobalt Strike	Percent of customers affected : 1.5%
August rank : ⬇ 3	Threat name: Mimikatz	Percent of customers affected : 1.3%
August rank : ⬆ 4	Threat name: Yellow Cockatoo	Percent of customers affected : 0.9%
August rank : ⬆ 5*	Threat name: Adload	Percent of customers affected : 0.7%
August rank : ⬇ 5*	Threat name: SocGholish	Percent of customers affected : 0.7%
August rank : ⬇ 7	Threat name: Gamarue	Percent of customers affected : 0.6%
August rank : ⬆ 8*	Threat name: Empire	Percent of customers affected : 0.5%
August rank : ⬆ 8*	Threat name: Metasploit Framework	Percent of customers affected : 0.5%
August rank : ➡ 8*	Threat name: Rose Flamingo	Percent of customers affected : 0.5%

⬆ = trending up from July
⬇ = trending down from July
➡ = no change in rank from July

*Denotes a tie

Rose Flamingo rises into top 10 threat rankings

Rose Flamingo is a new activity cluster that we've identified emerging over the past several months. We name new activity clusters when we observe overlap across various detections that we are unable to successfully associate to any known threats named by the community. Rose Flamingo's initial access occurs via file-sharing websites purporting to provide free or "cracked" software. The ZIP files downloaded from these websites have enticing strings in their names like `free`, `key`, `download`, `license`, `latest`, `iso`, or `crack`, and contain a TXT file with a password for an additional nested ZIP file. The nested ZIP file is where the trouble really begins, as it contains the initial loader that delivers additional malicious payloads. We observed a variety of payloads, from coinminers to infostealers and even a single instance of ransomware. Other researchers from Sophos and BitDefender have observed activity that overlaps with what we identify as Rose Flamingo, and we plan to release further details on it in the future as this threat emerges.

TA551 prevails as the most prevalent threat thus far in 2021

TA551, also known as Shathak, is a threat group that uses large-scale phishing campaigns to deliver additional malware payloads. It continued to surge ahead in prevalence over the past month, overtaking Cobalt Strike as the most prevalent threat in August as well as 2021 overall. So far this year, nearly 10 percent of all Red Canary customers have encountered a TA551 detection. BazarBackdoor was TA551's payload du jour for most of August, though we were fortunate to catch this threat early enough that we did not encounter any cases of BazarBackdoor activity last month. Credit for that early intervention goes to those implementing strong mitigating controls, including restricting access to Office macros and blocking traffic to new domains. TA551 was also the #1 most prevalent threat Red Canary observed in 2020, and fortunately the same detection opportunities we shared in our Threat Detection Report are still effective in catching this threat.

Adversaries continue to exploit enterprise applications for initial access

In August 2021, Red Canary observed adversaries exploiting vulnerabilities in WebLogic and Confluence to carry out a variety of follow-on actions in multiple environments. Given the frequency with which vulnerabilities are disclosed and the ease with which adversaries can exploit newly reported weaknesses, particularly in common applications, Red Canary focuses on identifying and detecting the behavior we observe surrounding exploitation of a vulnerability, and we recommend others take this approach as well. Understanding the threats we see and the ways in which adversaries operate in compromised networks allows us all to protect our networks from malicious activity regardless of the means by which the environment is accessed.

WebLogic

A handful of attacks we observed last month involved tactics, techniques, and procedures (TTP) that overlap with those used by an adversary known as Prophet Spider, a threat group named by CrowdStrike that is known to compromise vulnerable WebLogic servers and hand off access to ransomware operators. In campaigns we saw (which were consistent with CrowdStrike's excellent reporting), the adversary compromised vulnerable WebLogic instances, dropped a web shell on victims' endpoints, and installed various tools. We also identified behavior consistent with ransomware precursor activity in one instance.

Detection opportunity: Certificate Utility Authority decoding data

This detection opportunity helped us identify Base64-encoded data that was stored in a `.txt` file being decoded and written to a `.jsp` web shell file.

Process = `certutil.exe`
&
Command_line includes `decode`

You can test the efficacy of this detection opportunity by running this Atomic Red Team test in Command Prompt

Confluence

We also saw adversaries exploit a recently disclosed vulnerability in Confluence (CVE-2021-26084) and use a variety of tools in an attempt to mine cryptocurrency from victims. Activity we observed was consistent with open source reporting on threats exploiting this vulnerability.

Detection opportunity: Redirected Base64-encoded commands into bash

This Linux detection opportunity helped us identify execution of a Base64-encoded command that was redirected into `bash` using brace expansion syntax. This command initiated the download of z0miner.

Process = `bash`
&
Command_line includes `base64 -d`
&
Command_line includes `bash`

You can test the efficacy of this detection opportunity by running this Atomic Red Team test in `sh!`.

"Crypters" become newest "as-a-Service" threat

In the past few months, we've tracked multiple "Crypters-as-a-Service" (CaaS) that facilitate the delivery of malware through various PowerShell obfuscation methods. The CaaS model is another addition to the growing market of tools and services geared toward adversaries with lower technical sophistication. These crypters lower the barrier of entry for RAT infections, and tracking them helps us more accurately track use of the crypter versus the RAT.

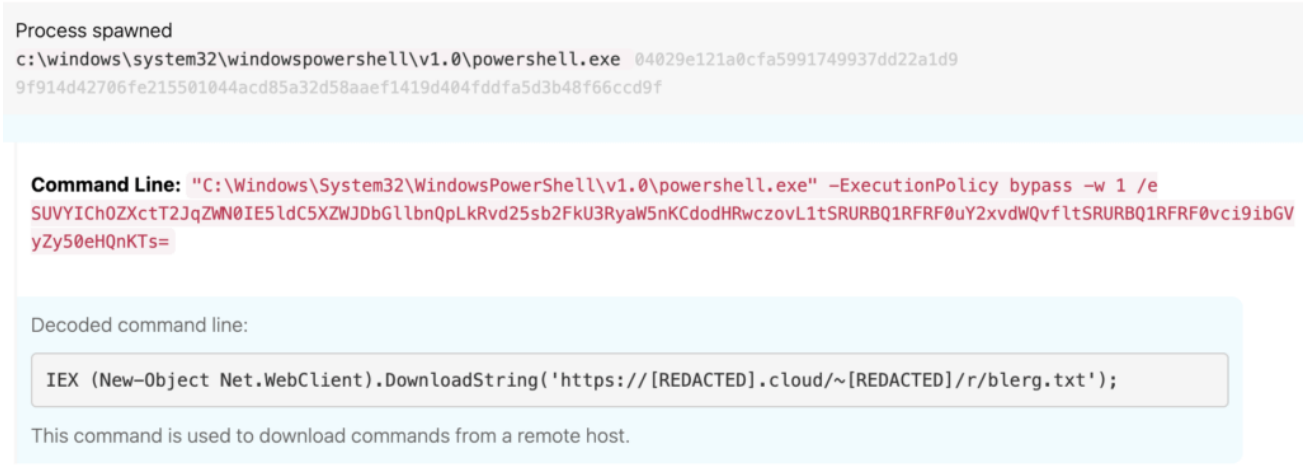
The first crypter we've been tracking is called "HCrypt." According to our own observations and public reporting, adversaries using HCrypt typically drop RATs such as ASyncRAT, Quasar RAT, and LimeRAT. Adversaries leveraging HCrypt have been observed gaining initial access via phishing attachments, often leveraging image files (IMG or ISO) containing a script (VBS or JS) that launches HCrypt. The malicious script downloads an additional script hosted on various publicly accessible sites including archive, cloud hosting, code repositories, and paste sites. This execution chain ultimately leads to a RAT infection.

Another crypter we've been tracking is called "Snip3," which was first documented in May 2021. It drops similar RATs to those we observed with HCrypt, including AsyncRAT, Agent Tesla, and Revenge RAT.

Detection opportunity: PowerShell command contains "DownloadString"

This detection opportunity helped us identify HCrypt's Base64-encoded PowerShell command to download an additional obfuscated PowerShell script.

Process = `powershell`
&
Command_line includes `downloadstring`



You can test the efficacy of this detection opportunity by running this Atomic Red Team test from PowerShell.

Look familiar?

If you've run into any of these behaviors on your environment, let us know!

Related Articles

Detection and response

ChromeLoader: a pushy malvertiser

Detection and response

Intelligence Insights: May 2022

Detection and response

The Goot cause: Detecting Gootloader and its follow-on activity

Detection and response

Marshmallows & Kerberoasting

Subscribe to our blog