Intelligence Insights: November 2021

Compromised NPM package distributes cryptominer, TR delivers SquirrelWaffle, and Gamarue rises up the threat ranks.

THE RED CANARY TEAM

Originally published November 18, 2021. Last modified June 7, 2022.

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 share a public version of it with the broader infosec community.

Highlights

In October 2021, we observed the same threats we've grown accustomed to seeing each month. Though the relative rankings largely remained the same, the volume of activity associated with **Yellow Cockatoo** and **TA551** respectively decreased. Despite its ranking, TA551 affected approximately 1.1% of customers in October, compared to 2.5% of customers in September. Similarly, Yellow Cockatoo affected approximately 1.1% of customers in October, compared to 2.7% in September. Lest you get complacent and think these prevalent threats are waning, the end of the month saw a surge from a previously prolific phisher pushing a familiar foe: **Qbot** is on the rise again, propelled by TR campaigns leveraging SquirrelWaffle. More on that and other interesting insights from the month are below.

As we've done for the past few months, we again looked at the 10 most prevalent threats encountered in the environments that Red Canary monitors. These prevalence rankings are based on the number of unique customer environments in which we observed each threat. For more information on any of these threats, check out **Intelligence Profiles**. Here's how the numbers shook out for October 2021:

TOP THREATS IN OCTOBER 2021

October rank : ↑ 1
Threat name: Mimikatz
Percent of customers affected : 1.6%

October rank : ↓ 2*
Threat name: Yellow Cockatoo
Percent of customers affected : 1.1%

October rank : → 2*
Threat name: TA551
Percent of customers affected : 1.1%

October rank : ↑ 2*
Threat name: Gamarue
Percent of customers affected : 1.1%

October rank : → 5*
Threat name: Cobalt Strike
Percent of customers affected : 1.0%

October rank : ↑ 5*
Threat name: Impacket
Percent of customers affected : 1.0%

October rank : ↑ 7*
Threat name: Qbot
Percent of customers affected : 0.7%

October rank : ↓ 7*
Threat name: SocGholish
Percent of customers affected : 0.7%

October rank : → 9*
Threat name: Metasploit
Percent of customers affected : 0.5%

October rank : ↑ 9*
Threat name: Wannacry
Percent of customers affected : 0.5%

↑ = trending up from previous month
↓ = trending down from previous month
→ = no change in rank from previous month

GET A DEMO

NodeJS with a side of XMRig

Third-party developer libraries and packages are an inescapable part of modern development, and the compromise of one package can cascade and affect multiple subsequent packages that depend on a single one. While fallout from a compromise of a popular NPM package last month appears relatively limited, the incident was a stark reminder of how adversaries can exploit organizations' reliance on trusted development tools. In fact, as we're getting ready to publish this, we're investigating a new potentially compromised package.

In October 2021, Red Canary identified a compromised package in NPM, a package distribution and management utility for JavaScript libraries. The compromised version of the package, `ua-parser-js`, distributed an XMRig cryptominer to Windows and Linux systems, as well as an infostealer (likely DanaBot) to Windows systems. Though the package is downloaded nearly 8 million times each week and the impact could have been widespread, GitHub quickly issued an **advisory warning** users that updating that package, or anything that depended on it, would initiate malicious behavior on affected systems.

In this case, we detected the compromised version of `ua-parser-js` with detectors designed to identify the cryptominer and infostealer it distributed. Detection opportunities for this category of threat inherently depend on which malware a poisoned package contains.

Detection opportunity: **Certutil downloading a file**

This detection opportunity will identify instances of Certificate Authority Utility (`certutil.exe`) with command-line arguments to download an arbitrary file. This behavior is commonly observed across multiple threats and is one reliable way adversaries use to download tools on Windows.

process == `certutil.exe`
&&
command_line_contains == `urlcache`

When TR delivers SquirrelWaffle, ransomware precursors may soon follow…

In late October 2021, Red Canary observed an uptick in detections involving **TR** (a delivery affiliate) and **SquirrelWaffle**. In some cases where we detected TR delivering SquirrelWaffle, we observed additional payloads and domain reconnaissance beginning within minutes. The short dwell time, combined with **recent external reporting** that suggests new TR tradecraft can bypass certain email protections, highlights the need to detect and respond to these behaviors in near real time to avoid late-stage activity such as ransomware.

Recent initial access tradecraft may allow adversaries to bypass certain protections provided by secure email gateways, increasing the odds that a malicious email is delivered to users' inboxes. In early November, security researchers **reported** that TR used compromised, on-premises Exchange servers to send malicious emails to potential victims. As context, successful exploitation of Microsoft Exchange on-premises products **enables** system access, control of an enterprise email server, and **access to enterprise email accounts**. This access effectively allows an adversary to send and receive email from a victim's account with the legitimacy of a trusted, internal sender.

Decreased dwell time underscores the criticality of detecting and responding to ransomware precursor activity quickly. In one incident, operators executed Cobalt Strike and BloodHound—hallmark ransomware precursors—only 75 minutes after a user first opened the malicious XLS phishing lure that initiated SquirrelWaffle. Short dwell times necessitate a clear understanding of adversary behavior and a robust toolbox of detection analytics to identify this behavior.

Detection opportunity: **Excel spawning Regsvr32**

This detection opportunity will identify instances of `regsvr32.exe` spawning as a child process of Microsoft Excel. This behavior is commonly observed in malicious documents with macros or Dynamic Data Exchange (DDE) execution, notably SquirrelWaffle XLS documents delivered by TR.

parent_process == `excel.exe`
&&
process == `regsvr32.exe`

With a twinkle in its eyes, Gamarue makes the ascent

While most of us were reaching for our favorite pumpkin spice latte this past month, Gamarue's spot in our rankings suggests that many others opted to reach for their thumb drives instead. Gamarue is a malware family used as part of a botnet. Some variants of Gamarue are worms and frequently spread via infected USB drives. Gamarue has also been used to spread other malware, steal information, and perform other activities such as click fraud. This malware was first seen more than 10 years ago and evolved into multiple variants before the operator was **arrested in 2017**.

Though Gamarue is no longer actively developed, it remains a pervasive threat. This highlights the notion that even if a threat is **no longer active**, it still warrants consideration from defenders tasked with responding to threats and building new detection logic.

Detection opportunity: **Rundll32 Gamarue CLI**

While we love to focus on detection opportunities that can identify multiple different threats by identifying uncommon types of behavior, this detection opportunity focuses on activity that is specific to multiple different Gamarue variants. Below you will find various examples that can be used to identify these variants executing.

1. `\--_--_--_-__--_-__-__-__-_--__---_--_--_--_.--_--_--_-__--_-__-__-__-_--__---_--_--_--_,LFoRW4dX01fM8FeX`
2. `\_--_____--__----__--____---_----.{0B5C7B4B-7F44-02BE-99D4-8C4E124562AD},qwertyuiop123456`
3. `\\\\\\\\\\\~%%@@~%%@@~%%@@~.2,1abcDEfgHIJ2klM4`

In conjunction with this detection opportunity, you may be able to identify the name of an infected thumb drive that was plugged into the endpoint by looking for registry modifications to **UserAssist** registry keys containing the ROT13 encoded string `.yax` at the same time. These registry values can be decoded to look something like `f:\usb drive (8gb).lnk`, which may be indicative of a USB drive being the culprit.

process == `rundll32.exe`
&&
command_line_matches == `\\[-_.]+\,\w+`

process == `rundll32.exe`
&&
command_line_matches == `\\[-_]+\.\{[A-Z0-9-]{36}\}\,\w+`

process == `rundll32.exe`
&&
command_line_matches ==`\\+[~$%@]+\.\d\,\w+`

Detection opportunity: **Rundll32 spawning Explorer**

This detection opportunity hinges on the likelihood of `rundll32.exe` spawning `explorer.exe`. Red Canary often observes Gamarue spawning the `explorer.exe` process in an unusual way.

parent_process == `rundll32.exe`
&&
process == `explorer.exe`

Detection opportunity: **Msiexec No CLI + External Netconn**

As we mentioned in our **2021 Threat Detection Report**, Gamarue can still be detected by identifying instances of the Windows Installer (`msiexec.exe`) into which it has been injected. This type of activity can be identified by creating a detection analytic that focuses on instances of Msiexec that have no associated command-line options or an external network connection.

&&
`has_external_netconn?`

**Note: Double quotes (“”) within the command line means null.*

New opportunities for detecting ransomware precursors

In October, we observed Conti and Lockbit affecting multiple customer environments. Fortunately, there are several opportunities to detect precursor behavior for these threats.

Conti precursor activity

In October, we observed several **new Qbot TTPs** in environments ultimately encrypted with Conti. Notably, we saw Qbot inject into Microsoft Synchronization Center (`mobsync.exe`) and drop Conti DLLs. Additionally, we saw Qbot inject into Windows Error Reporting (`werfault.exe`) with no command-line parameters. Following this, the adversary used the `xcopy` utility to copy the malicious DLLs to different locations on the system. There are multiple opportunities to detect this activity in your environment:

Detection opportunity: **Mobsync creating unusual DLL files**

This detection analytic will identify an unusual file modification stemming from the `mobsync.exe` process. We determined this file was Conti ransomware in one incident.

process == `mobsync.exe`
&&
file_modification_create == `*.dll`

Detection opportunity: **Werfault spawning with no command-line parameters**

This detection analytic will identify unusual activity originating from the `werfault.exe` process. Werfault typically spawns with command-line parameters when a process crashes, providing the program with input to create an error report.

process == `werfault.exe`
&&
command_line == **“”**

Detection opportunity: **Xcopy moving files from Group Policy Object (GPO) storage folder**

Qbot created malicious files within the GPO storage folder during execution. Then, it used the Extended Copy Utility (`xcopy.exe`) to copy malicious DLLs, including Conti. The following analytic will identify this activity:

process == `xcopy.exe`
&&
command_line_contains == `\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\`
&&
file_modification_create == `*.dll`

**Note: `31B2F340-016D-11D2-945F-00C04FB984F9` is the default domain policy GUID*

Lockbit precursor activity

During a recent Lockbit infection, the operators used PsExec to launch a batch script, which initiated several commands designed to prepare the environment for encryption. The batch script displayed the following actions:

- set antivirus exclusion paths for `C:\Programdata\` and `C:\Windows\` that allowed malicious binaries to exist in these paths without interference
- deleted the Windows Defender service
- disabled Windows Defender, User Account Control (UAC), and Windows Recovery
- turned off all firewall rules
- cleared multiple System and Security logs

The defense evasion and system recovery commands initiated by the script offer multiple detection opportunities.

Detection opportunity: **Disabling Windows Recovery via bcedit**

In combination with the other commands witnessed in the same timeframe, the use of the Boot Configuration editing tool (`bcdedit.exe`) to set specific recovery options helped us identify malicious activity.

process == `bcdedit.exe`
&&
Parent_process == (`“rundll32.exe”` || `“regsvr32.dll”`)
&&
command_line_contains == `“recoveryenabled No”`

Detection opportunity: **Wevtutil clearing System and Security logs**

The Windows Event Log Utility Tool (`wevtutil.exe`) process deleted both System and Security event logs. This behavior is atypical in most environments.

process == `wevtutil.exe`
&&
command_line_contains == `cl`
&&
(command_line_contains == `Security`
||
command_line_contains == `System`)

Detection opportunity: **Netsh turning off all firewall rules**

Setting all of the system firewall rules to a state of “off” should be considered suspicious and investigated further. While this may be a “normal” system administration function in some cases, it merits close review when observed with other activity associated with Lockbit.

process == `netsh.exe`
&&
command_line_contains == `advfirewall set allprofiles state off`