RESOURCES • BLOG

THREAT INTELLIGENCE

Intelligence Insights: October 2021

THE RED CANARY TEAM

Originally published October 21, 2021. Last modified April 30, 2024.

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

September brought some changes in our threat rankings, with Yellow Cockatoo soaring to the top of the list. While Yellow Cockatoo has been a mainstay in the top 10 threats for months, its activity increased dramatically in September, impacting more customers last month than in the previous three combined. The rest of the top seven is comprised of the usual suspects, but the back end of the list included several threats that had not cracked the top 10 all year. BazarBackdoor and Zloader, #8 and #9, are notable **ransomware precursors** that we consistently see. Conti tied for #9 due to several full-blown **Conti ransomware** incidents observed through short-term incident response engagements.

For brevity, we included these three ninth-place ties in the table. However, there were actually six more threats that tied for ninth in the September prevalence rankings. These threats include top 10 regulars **Qbot** and Metasploit, along with common Mac threats **Shlayer**, Bundlore, and Adload, as well as the Ippedo worm.

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

TOP THREATS IN SEPTEMBER 2021

AUGUST RANK	THREAT NAME	PERCENT OF CUSTOMERS AFFECTED
↑ 1	**Yellow Cockatoo**	2.7%
↓ 2	**TA551**	2.5%
→ 3	**Mimikatz**	1.5%
↑ 4	SocGholish	1.4%
↓ 5	**Cobalt Strike**	1.3%
↑ 6	Impacket	1.2%
→ 7	**Gamarue**	0.7%
↑ 8	Zloader	0.5%
↑ 9*	**BazarBackdoor**	0.4%
↓ 9*	Rose Flamingo	0.4%
↑ 9*	Conti	0.4%

↑ = trending up from previous month
↓ = trending down from previous month

*Denotes a tie

Yellow Cockatoo takes flight above the rest

In September 2021, we observed a rise in the number of detections for **Yellow Cockatoo**, an activity cluster involving the execution of a .NET remote access trojan (RAT) that runs in memory and drops additional payloads. Not only did the volume of activity we observed increase substantially (as evidenced by its rise to the top of our charts), Yellow Cockatoo also adopted a new installation mechanism chronicled **here** by researchers at Morphisec and outlined below.

- **Search engine redirects enable Yellow Cockatoo operators to carry out seemingly targeted social engineering attacks at scale.** Initial access by Yellow Cockatoo often occurs via a search engine redirect that appears to direct a user from a legitimate search engine to a site that downloads a malicious binary bearing the victim's search query as its name (for example: `this-is-my-search-query.msi`). Because potential victims are directed to a site based on a search they initiated, they may be more inclined to engage with its content. Though many adversaries craft tailored attacks and leverage familiar themes, Yellow Cockatoo is unique in its ability to dynamically "customize" its attacks based on victims' real-time searches.
- **In September 2021, Yellow Cockatoo adopted MSI files as an installation mechanism.** Last month, Yellow Cockatoo began using MSI installers rather than previously observed .exe files. This resulted in different behaviors, including `msiexec.exe` execution of a compressed GUID followed by the creation of PS1 scripts.
- **These MSI installers generated a consistently recognizable PowerShell command line.** This command line is an artifact generated when a malicious MSI installer is created with **Advanced Installer**. While we saw this in recent Yellow Cockatoo detections, it is not unique to Yellow Cockatoo because any MSI installer created with this tool would exhibit this behavior. As one example:

```
"C:\Users\[name]\AppData\Local\Temp\msi4DB2.txt" -scriptFile "C:\Users\
[name]\AppData\Local\Temp\scr1EA7.ps1" -scriptArgsFile "C:\Users\
[name]\AppData\Local\Temp\scr4FA1.txt" -propSep " :<->: " -testPrefix
"_testValue."
```

Yellow Cockatoo continued to write malicious `.lnk` files into the startup directory. As we've seen in activity detected prior to September 2021, in recent detections, Yellow Cockatoo malware created an `.lnk` file in `startup` to establish persistence in compromised environments:

```
c:\users\[redacted]\appdata\roaming\microsoft\windows\start
menu\programs\startup\a6ee8c157724e7945bfcd9eb64fa3.lnk
```

There are multiple opportunities to detect this threat and harden your environment.

Detection opportunity: **PowerShell writing startup shortcuts**

We frequently observe adversaries using PowerShell to write malicious `.lnk` files into the startup directory to establish persistence. Accordingly, this detection opportunity is likely to identify persistence mechanisms in multiple threats. In the context of Yellow Cockatoo, this persistence mechanism eventually launches the command-line script that leads to the installation of a malicious DLL:

process_name == `powershell.exe`

&&

process_command_line_contains == `appdata`

&&

filemod_path_contains == `start menu\programs\startup`

filemod_extension == `.lnk`

*You can test the efficacy of this detection opportunity by running **this Atomic Red Team test** in PowerShell with elevated privileges.*

To harden your attack surface against the search engine redirects commonly used by Yellow Cockatoo, we recommend taking steps to prevent access to malicious domains and other malicious content on the internet. This could involve configuring your web proxy to block newly registered and low reputation domains (e.g.,`*.tk`, `*.top`, and `*.gg`) as well as blocking ads.

ZLoader juggles discs

In September, Red Canary and external **researchers** observed a change in how adversaries are delivering ZLoader payloads: hijacking Google Adwords to inject malicious content into advertisements. Although this tactic isn't exactly novel, it is a new means of distribution for Zloader. Additionally, Red Canary observed **new modifications** to the ZLoader delivery process involving Windows Installer Package `.msi` payloads. Interestingly, the adversaries behind Yellow Cockatoo modified their tactics to incorporate `.msi` payloads for the first time this month as well, but we are uncertain why either has opted to make such a change.

In our analysis of these ZLoader `.msi` payloads, we found that the packages integrate the delivery of a legitimate remote monitoring management (RMM) utility known as Atera. Malware dropping Atera is cause for concern because adversaries have deployed **AteraAgent** as a ransomware precursor. If you do not utilize Atera services within your organization, consider taking steps to **detect and prevent** network communications to Atera infrastructure, as it may be indicative of malicious activity. If you are interested in detecting threats utilizing RMM software, you can read more about this type of activity in one of our latest **blogs**.

Detection Opportunity: **Atera Agent Regmod**

This detection opportunity will identify any registry modifications consistent with Atera Agent utilization:

registry_modification_path_contains == `ATERA Networks`

We also observed adversaries distributing later variations of ZLoader as a mountable Virtual Hard Disk `.vhd` file. Malicious use of `.vhd` files is still uncommon, though this shift is consistent with a broader trend of adversaries leveraging other **virtual disc formats**, like `.img` and `.iso` files, to encapsulate payloads and evade security controls. Though we do not know exactly why adversaries have refrained from adopting the `.vhd` format more, native support for the `.vhd` format is a relatively **new** addition as of Windows 8. It may only be a matter of time until we see additional adversaries opting to use the format more often.

Detection Opportunity: **Browser Writing VHD**

This detection opportunity will identify most enterprise-approved browsers writing VHD files to disk:

process_name == (`chrome.exe` || `firefox.exe` || `microsoftedge.exe` || `microsoftedgecp.exe` || `msedge.exe`)

&&

filemod_extension == `.vhd`

BlackByte bites back against defenses

This month, we observed the BlackByte ransomware variant impacting a customer environment in some unique ways. BlackByte is a relatively new variant; it first appeared in public reports around July 2021, and its operators launched a new extortion leak site in September. Some interesting BlackByte TTPs that we've observed include:

- **Print bombing:** Though not a new technique (Ryuk operators used it previously), print bombing is not especially common. The technique involves using discovered network printers to print physical copies of a ransom note. In this case, the scheduled task stored the command to initiate the print jobs.
- **Shadowstorage deletion:** The BlackByte sample we observed leveraged the `vssadmin resize` method of **shadow copy deletion** in which adversaries change the size of shadow copies, resulting in their deletion. We have also seen this method used by Conti, Ryuk, and Clop. This behavior would have theoretically been intercepted by the Raccine tool. However, BlackByte incorporated a backup method of deletion by using PowerShell to iterate through the `Win32_ShadowCopy` WMI objects and delete them.

Detection Opportunity: **Vssadmin Resizing shadowstorage**

This detection opportunity helps identify attempts at malicious resizing of shadowstorage backup files:

process = `vssadmin`

&

Despite BlackByte's recent emergence, other ransomware operators have used the same techniques outlined above. As new ransomware families appear almost daily, the same **prevention, detection, and response** approaches remain relevant across multiple groups. Though ransomware is very detectable, identifying the **precursor activity** associated with ransomware continues to be the best method for preventing widespread infections from impacting enterprises.

Conti's message is clear: Ransomware isn't gone

Since our visibility into ransomware mostly comes from engagements with partners, it's rare that any ransomware family itself makes it into the top 10. We focus on detecting ransomware precursors to avoid ransomware itself! However, in September, Conti tied for our #9 threat due to multiple short-term incident response engagements. This is notable in part because of recent news reports and messaging that ransomware is declining. While there is limited evidence that there may have been a **slight decline** over the summer, ransomware is clearly not gone.

Conti was busy compromising multiple organizations in September, and DHS CISA released a **Joint Cybersecurity Advisory** outlining its TTPs. As we noted with BlackByte, Conti operators use TTPs similar to that of other ransomware groups. One **interesting TTP** from Conti operations is the use of the RMM utility Atera (as discussed above) to establish persistence, which supplemented initial Cobalt Strike beacons as an additional measure to evade further detection.

LOOK FAMILIAR?

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

→

RELATED ARTICLES

THREAT INTELLIGENCE

Intelligence Insights: October 2024

THREAT INTELLIGENCE

Intelligence Insights: September 2024

THREAT INTELLIGENCE

Recent dllFake activity shares code with SecondEye

THREAT INTELLIGENCE

Intelligence Insights: August 2024

Subscribe to our blog

You'll receive a weekly email with our new blog posts.

First Name

Last Name

Email Address

SUBSCRIBE >

GET A DEMO >

What's New?
Plans

Protect Your Users' Email, Identities, and SaaS Apps
Protect Your Cloud
Protect Critical Production Linux and Kubernetes
Stop Business Email Compromise
Replace Your MSSP or MDR
Run More Effective Tabletops
Train Continuously for Real-World Scenarios
Operationalize Your Microsoft Security Stack
Minimize Downtime with After-Hours Support

RESOURCES

View all Resources
Blog
Integrations
Guides & Overviews
Cybersecurity 101
Case Studies
Videos
Webinars
Events
Customer Help Center
Newsletter

PARTNERS

Overview
Incident Response
Insurance & Risk
Managed Service Providers
Solution Providers
Technology Partners
Apply to Become a Partner

COMPANY

About Us
The Red Canary Difference
News & Press
Careers – We're Hiring!
Contact Us
Trust Center and Security

GET A DEMO ›