RESOURCES • BLOG

THREAT INTELLIGENCE

Intelligence Insights: December 2021

THE RED CANARY TEAM

Originally published December 16, 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

Editor's note: We realize much of the cybersecurity community is focused on the Log4j vulnerability right now, and we're tracking that too. The post-exploitation activity we've observed remains fairly low at this time, though that could change. While the Log4j vulnerability is undoubtedly important, we want to continue to release intelligence about all the other threats we've seen that are still impacting enterprises. Some of the threats in our top 10, such as **Cobalt Strike** and **Mimikatz**, have been observed in **activity following exploitation** of the Log4j vulnerability. This underscores the importance of continuing to track prevalent threats and entire chains of activity while also taking actions to remediate such a widespread vulnerability.

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. Here's how the numbers shook out for November 2021:

TOP THREATS IN NOVEMBER 2021

↑ 1	Impacket	1.9%
↑ 2*	**Cobalt Strike**	1.5%
↓ 2*	**Mimikatz**	1.5%
↑ 4	SocGholish	1.3%
↑ 5	**Qbot**	1.1%
↓ 6	**TA551**	1.0%
↑ 7	Adload	0.9%
↑ 8*	TR	0.8%
↑ 8*	SquirrelWaffle	0.8%
↓ 10*	**Gamarue**	0.7%
↑ 10*	Ursnif	0.7%

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

*Denotes a tie

Qbot continued to climb the ranks on the back of TR phishing campaigns leveraging SquirrelWaffle. Both TR and SquirrelWaffle cracked our top 10 for the first time this month. If you're wondering why the payload (Qbot) is more prevalent than the initial access (TR), there are a few explanations. One is that there are multiple campaigns leading to Qbot. While TR is prolific, it is not the only source of the Qbot we see. Another reason that we sometimes see more later-stage activity rather than initial access is that it's an artifact of onboarding customers during incident response. In many cases, our visibility into an environment begins in the middle of the attack chain —when the command and control bots (i.e., Qbot) are actively running but the ephemeral initial access has already run its course.

While it didn't make our top 10, we saw more detections* for BazarBackdoor than we've previously seen in any single month. Phishing campaigns delivered BazarBackdoor every Tuesday and Wednesday for the first three weeks of November. Despite this pattern in the timing, we observed variations in the phishing affiliate delivering the payload. For example, one affiliate that we had historically tied to Bazar recently began delivering Emotet as well. See the section"Guess who's back…" below for details.

*This increase applies both to the number of customer environments and the number of individual detections.

Conspicuously absent from this list is Yellow Cockatoo, which previously topped our charts. After a meteoric rise in late summer and early fall, Yellow Cockatoo was the most prevalent threat we saw in Red Canary customers in September. This prolific pest perpetuated its preponderance throughout most of October, then vanished suddenly. This observation is consistent with the timeline of reporting from a researcher, going by the handle "SquiblyDoo," who closely monitors Yellow Cockatoo activity. Squiblydoo's research trail appears to have gone cold after posting **a blog** in mid-October with updates on changes in Yellow Cockatoo's TTPs. Red Canary continues to monitor for signs of new activity and will update our coverage if—and when—anything changes.

Guess who's back, back again… Emotet's back, tell a friend…

Months after a **coordinated effort** disrupted their infrastructure and operations, Emotet has returned and they're changing things up. For the first time this month, we

- **In November 2021, Red Canary observed Emotet delivered via AppX, a type of installer bundle used to distribute common Windows applications.** In these cases, victims interacted with a website spoofed to resemble an installer for Adobe PDF software, where they downloaded an AppX bundle containing an Emotet file.
- **Emotet activity in November also involved previously known delivery mechanisms.** Much of the other Emotet activity we saw resembled variations on Emotet campaigns of the past. In these cases, documents sent as attachments via email contained PowerShell code written to download Emotet payloads, which used the export Control_RunDLL for execution. Though we did not observe this activity firsthand, in mid November, security researchers observed Trickbot malware infections deploying Emotet payloads.
- **This evolving tradecraft complicates efforts to track and attribute activity.** In the case of the AppX bundles, Emotet appeared to use the same resources that were used by BazarBackdoor for deployment earlier in November. Since Red Canary observed the same activity and resources used by both families, we decided to track the AppX bundle deployment activity cluster under a separate name: Ultramarine Wren.

As Emotet evolves and we observe its use in different activity clusters, we continue to track changes in behavior and corresponding ways to detect that behavior.

Detection opportunity: **Rundll32 execution with a unique function**

process_ name == `rundll32.exe`
&&
command_line_contains == `Control_RunDLL`
&&
command_line_ does_ not_ contain == `shell32`

Recent increase in websell activity likely stems from exploitation of ADSelfService Plus RCE vulnerability

Over November, Red Canary observed an increase in detections involving webshells. Further analysis suggests that many of these were likely the result of the exploitation of **CVE -2021-40539**, a vulnerability in ADSelfService Plus. ADSelfService Plus is a common password management and single sign-on (SSO) solution. Exploitation of this vulnerability can enable a range of nefarious follow-on activity, and multiple operators are reportedly using this exploit in the wild. We are tracking behaviors related to known compromises and recommend that customers using ADSelfServicePlus apply the **patch issued by ManageEngine**.

Researchers at Synactiv outlined in-the-wild use of tradecraft involving this vulnerability that allowed Red Canary to identify a specific behavior consistently related to this attack chain. We saw operators use the Java utility `keytool.exe` to move a recently installed webshell from an initial directory to a new location.

Detection opportunity: **Keytool.exe spawning Windows shell parent process**

```
parent_process_name==keytool.exe
&&
process_name ==(cmd.exe|| powershell.exe)
```

Failure to securely configure ADSelfService Plus can provide an adversary who

Admin. In turn, if an adversary were to exploit CVE-2021-40539, they would be given that level of permission and access to the Active Directory. To properly secure ADSelfService Plus and protect Active Directory accounts, we strongly recommend that customers refrain from running ADSelfService Plus with an elevated permissions account, such as **Domain Admin**. Instead, customers should use an unprivileged Active Directory account configured according to **guidance from ManageEngine.**

Based on our observations and public reporting from **CISA**, **Microsoft**, and **Palo Alto's Unit 42,** it is clear that post-exploitation activity varies across intrusions. We continue to track activity related to this threat and expand our detection coverage to account for new variations.

Detection opportunity: **Excel spawning WMIC**

parent_process_name == `excel.exe`
process_name == `wmic.exe`

Detection opportunity: **MSHTA execution without HTA file**

process name == `mshta.exe`
command_line_does_not_contain == `.hta`

As always, the assessments in this report represent our best thinking based on our current visibility. To this end, we welcome the receipt of conflicting or contradictory

LOOK FAMILIAR?

RELATED ARTICLES

THREAT INTELLIGENCE

Intelligence Insights: October 2024

THREAT INTELLIGENCE

Intelligence Insights: September 2024

THREAT INTELLIGENCE

Recent dllFake activity

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 ›