Intelligence Insights: April 2022

SocGholish falls from first place, Yellow Cockatoo rebounds in March, and Qbot campaigns leverage Windows Installer packages.

THE RED CANARY TEAM

Originally published April 21, 2022. 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

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 March 2022:

↑ 1	Impacket	1.5%
→ 2	**Mimikatz**	1.0%
↑ 2*	Yellow Cockatoo	1.0%
↑ 4*	**Cobalt Strike**	0.9%
↑ 4*	BloodHound	0.9%
↑ 6*	TR	0.7%
↑ 6*	Shlayer	0.7%
↑ 6*	**Emotet**	0.7%
↓ 9	**Qbot**	0.6%
↓ 10*	SocGholish	0.5%
↓ 10*	Gamarue	0.5%
↑ 10*	Bondat	0.5%

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

*Denotes a tie

Observations on trending threats

Overall threat volume remained steady in March, matching February's numbers with 14.3 percent of Red Canary customers encountering at least one detection associated with a named threat we track. **SocGholish** relinquished the top spot, retreating to the volume we typically saw throughout most of 2021. The return of **Yellow Cockatoo** in February fueled a

One newcomer you may have noticed in the middle of the pack is **BloodHound**, a tool we've been tracking for some time but only recently included in our metrics. While most of the BloodHound activity we see is related to pentesting or internal security teams, we have observed multiple threats leverage it in intrusions, some leading to ransomware. The numbers underlying the prevalence rankings do not distinguish red teaming from in-the-wild adversary activity. Therefore, the presence of popular tools employed by testers—such as **Impacket**, Mimikatz, **Cobalt Strike**, and **BloodHound**—are not surprising to see in this list.

MSI phishing lures deliver Qbot

In April 2022, researchers reported on new tradecraft associated with campaigns delivering **Qbot**, **a known ransomware precursor**. For the first time, researchers saw Qbot delivered via malicious Windows Installer (MSI) packages, suggesting that at least one subset of operators may be experimenting with new ways to evade victims' defenses. The recent Qbot campaigns leveraging Windows Installer packages are a deviation from past campaigns, where Qbot was delivered via malicious Microsoft Office macros. In both cases, the malicious dropper is delivered via phishing emails with password-protected ZIP archives sent as attachments.

Qbot is a mature malware threat with a range of capabilities that allow adversaries to conduct reconnaissance, move laterally on an infected network, exfiltrate data, or deliver other tools. Multiple adversaries have leveraged Qbot in compromises that quickly progressed to additional threats, including ransomware. Accordingly, it's critical to identify changes in Qbot behavior (and the procedures that adversaries use to deploy it) to enable quick detection and response to known infections.

This most recent change in tradecraft may be a response to ongoing efforts by defenders to disable certain macros by default. While multiple groups carry out operations involving Qbot, delivery tradecraft **has been consistent** over time, across various adversaries. In past campaigns, adversaries used weaponized Microsoft Office documents, which were embedded with malicious macros and delivered via phishing campaigns. Upon macro execution, victims downloaded and executed a Qbot payload, typically without knowing it. Though this was effective for several years, this approach largely relied on victims allowing the macros to run. Earlier this year, **Microsoft announced** that VBA macros obtained from the internet would be blocked by default. There is **some speculation** that changes to Qbot delivery mechanisms may be in response to this effort. Microsoft's move to allow **AMSI telemetry for XLM macros** likely means that adversaries are having to explore additional avenues for malware distribution, as previously reliable macro methods are becoming unavailable.

Detection opportunity: `regsvr32.exe` **spawning `explorer.exe` as a child process**

When Qbot payloads delivered via MSI execute successfully, `explorer.exe` will spawn from `regsvr32`. This detection opportunity identifies `regsvr32.exe` spawning `explorer.exe` as a child process.

```
process_is_likely == regsvr32
&&
```

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 ›

See Red Canary in action

Schedule your demo now

Get a Demo

→

Search

- Readiness Exercises
- Linux EDR
- Atomic Red Team™
- Mac Monitor
- What's New?
- Plans

- Get a 24×7 SOC Instantly
- Protect Your Corporate Endpoints and Network
- 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

- Guides & Overviews
- Cybersecurity 101
- Case Studies
- Videos
- Webinars
- Events
- Customer Help Center
- Newsletter

- Managed Service Providers
- Solution Providers
- Technology Partners
- Apply to Become a Partner

- Careers – We're Hiring!
- Contact Us
- Trust Center and Security

info@redcanary.com +1 855-977-0686 Privacy Policy Trust Center and Security

Cookies Settings