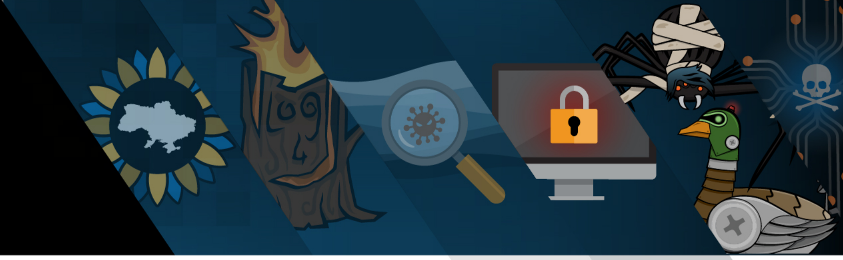
Cisco | Talos
2022 **YEAR IN REVIEW**



RANSOMWARE AND COMMODITY LOADERS

DOWNLOAD THE FULL REPORT HERE

RANSOMWARE THREAT LANDSCAPE

The ransomware space is dynamic, continually adapting to changes in the geopolitical environment, actions by defenders, and efforts by law enforcement, which increased in scope and intensity in 2022. This leads groups to rebrand under different names, shut down operations, and form new strategic partnerships. Cisco Talos observed several related trends across 2022.

Talos tracks more than a dozen ransomware-as-a-service (RaaS) groups **(Figure 1)**. Based on our findings, LockBit was the most active group in 2022, accounting for over 20 percent of the total number of dark web victim posts, closely followed by Hive and Black Basta. These findings point towards a greater democratization of ransomware adversaries, an overall change from previous years in which a select few groups monopolized the landscape. Ransomware affiliates are also no longer structured in silos and are now working across multiple groups, where actors with unique skill sets have more opportunities to support multiple campaigns and organizations.

There was also heightened friction throughout the community, as the war in Ukraine compelled many threat actors to choose sides in the conflict and direct their operations against pro-Russia or pro-Ukraine targets. The Conti RaaS group was among the most vocal, warning they would attack anyone who attempted to interfere with Russia's invasion. An individual with ties to Conti took revenge against the ransomware gang by leaking information, including the malware's source code and internal chats between affiliates. In another event, Talos became aware of the disclosure of a leaked builder for the LockBit 3.0 ransomware encryptor dubbed "LockBitBlack." The individual claiming responsibility is an alleged LockBit developer who, according to LockBit, claimed they were disgruntled with the group's payment structure.

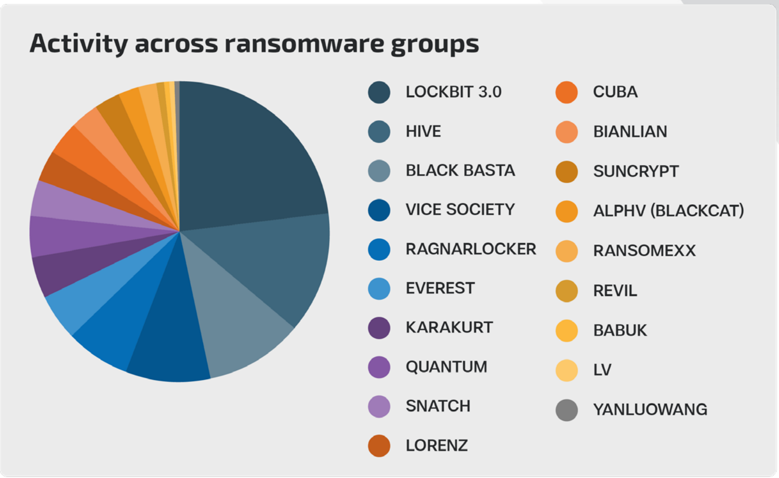


Figure 1. *Number of posts made to ransomware data leak sites tracked by Talos, January-October.*

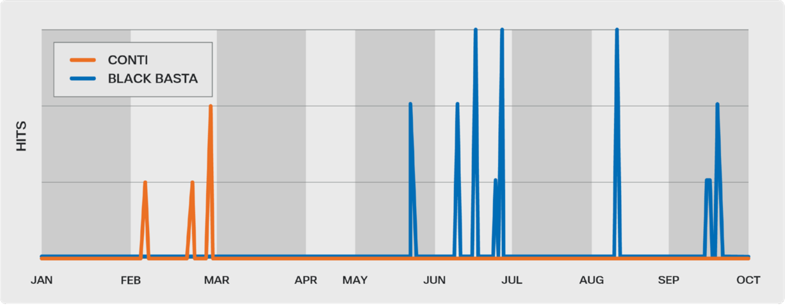


Figure 2: *Behavioral indicator detections in Secure Malware Analytics for Conti ransomware and Black Basta registry modifications.*

This type of friction is what often leads to ransomware gangs rebranding or new groups emerging. When Conti ceased operations and took its infrastructure offline, we saw a general drop in detections in our telemetry, but shortly thereafter, a re-brand of Conti dubbed "Black Basta" emerged. Researchers suggest the two groups have similar payment and leak websites and communication styles **(Figure 2)**.

COMMODITY LOADERS

Commodity loaders—commercial trojans that deploy second-stage malware—are a constant threat that continue to have a global impact. Initially developed as banking trojans designed to compromise entities for monetary gain, over time, they have adapted to greater

© 2023 Cisco and/or its affiliates. All rights reserved. | talosintelligence.com

RANSOMWARE AND COMMODITY LOADERS

security controls and developed into much more sophisticated threats. They now operate primarily as loaders with modular functions, allowing cybercriminals the flexibility to work with a range of open-source tools and newly developed malware. The four most active commodity loaders in 2022 were Qakbot, Emotet, IcedID, and Trickbot, according to our analysis of several network and endpoint telemetry sets **(Figure 3)**.

Although our telemetry detected activity associated with Trickbot, we assess much of this activity was likely detecting old, infected endpoints, as the malware operators have been inactive since early 2022. Similarly, Emotet, although still operational, remains significantly less active than it was before the botnet was dismantled in early January 2021 by law enforcement. Other malware has filled the void by becoming more popular, such as Qakbot and IcedID.

In one overarching trend in 2022 we observed, operators more frequently delivered Qakbot, Emotet, and IcedID using ISO, ZIP, and LNK file types, likely to circumvent Microsoft's efforts to block macros-enabled documents. In another trend, Talos observed Qakbot, Emotet, and IcedID operators downloading and launching malicious payloads using living-off-the-land binaries (LoLBins) found on victim environments. In some cases, the Qakbot and Emotet affiliates refined their attack sequence by experimenting with different LoLBins to improve their chances of staying undetected within an organization.

Although our telemetry detected activity associated with Trickbot, we assess much of this activity was likely detecting old, infected endpoints, as the malware operators have been inactive since early 2022. Similarly, Emotet, although still operational, remains significantly less active than it was before the botnet was dismantled in early January 2021 by law enforcement. Other malware has filled the void by becoming more popular, such as Qakbot and IcedID.

An in-depth review of each commodity loader is available in the full report.

Commodity Loaders

	Qakbot	IcedID	Emotet	Trickbot
Aliases	Quackbot, Qbot, Pinkslipbot	BokBot	Geodo, Heodo	N/A
Affiliations	Commodity malware likely developed by Eurasian cybercriminals	Unknown	Commodity malware developed by Mummy Spider, a Russian-aligned cybercrime group	Commodity malware developed by Wizard Spider, a Russian-aligned cybercrime group
Active since	2007	2014	2017	2016

Goals

- Gain initial access and establish persistence to facilitate further intrusion activities.
- Deploy next-stage malware, including ransomware.

Victimology

- Targets all sectors worldwide.
- Since the Russia-Ukraine war, Trickbot has threatened to retaliate against perceived attacks against the Russian people.

Notable TTPs

- Phishing, malspam, social engineering, vulnerability exploitation, data theft—such as financial data and credentials—and worm-like propagation.
- Highly modular, allowing operators to conduct a wide range of attacks.

Malware & tooling

- The malware variants both deploy, and are deployed by, various other malware families, including one another.
- Use commercial tools, such as Cobalt Strike, as well as LoLbins in various stages of the attack lifecycle.

Figure 3. *Commodity loaders threat matrix.*

© 2023 Cisco and/or its affiliates. All rights reserved.