Threat Intelligence

Ransomware: March 2022 review

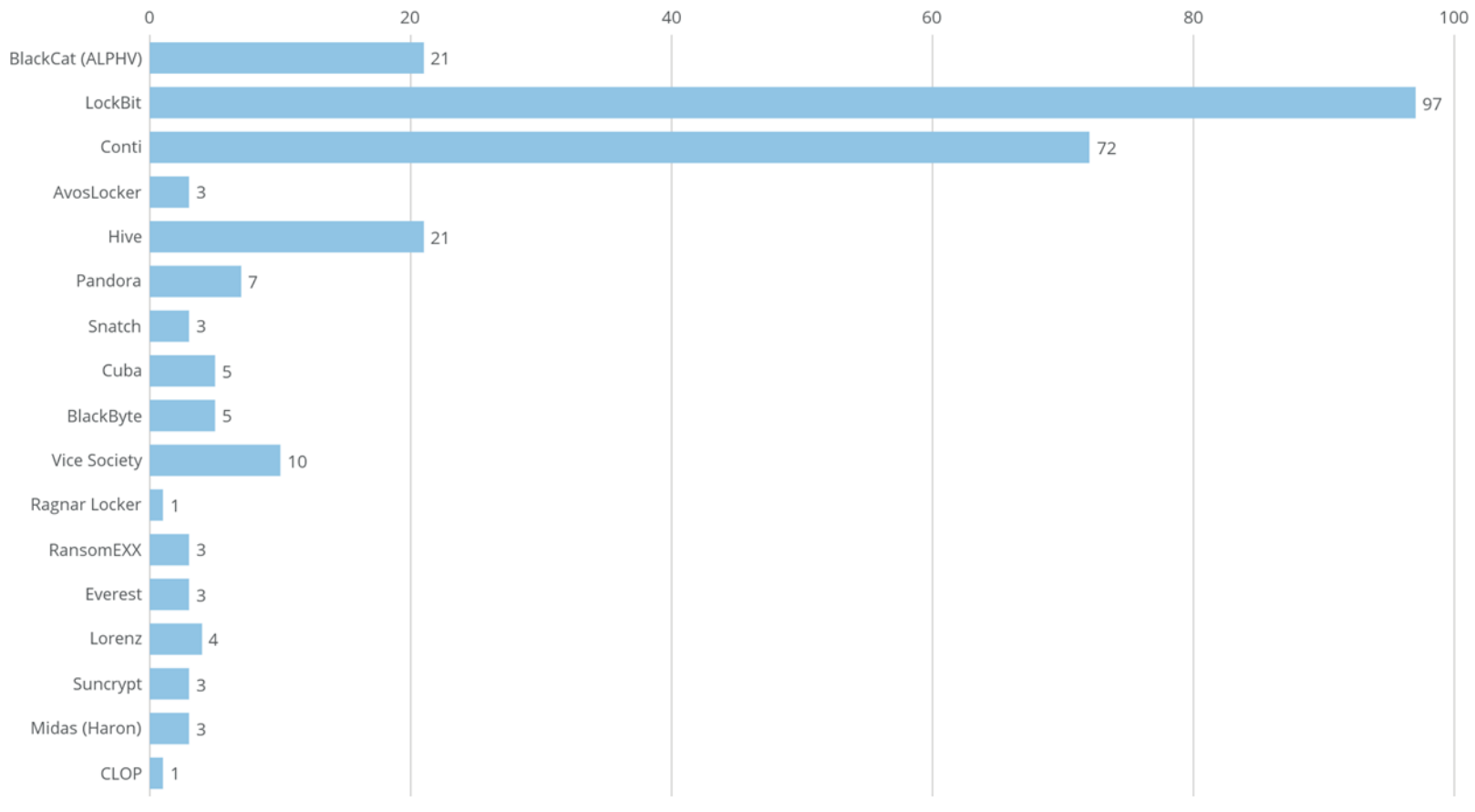
Posted: April 11, 2022 by Threat Intelligence Team

Get the latest information on ransomware trends with our monthly review.

The Malwarebytes Threat Intelligence team continuously monitors the threat landscape to stay on top of existing and emerging attacks. In this March 2022 ransomware review, we go over some of the most successful ransomware incidents based on both open source and dark web intelligence.

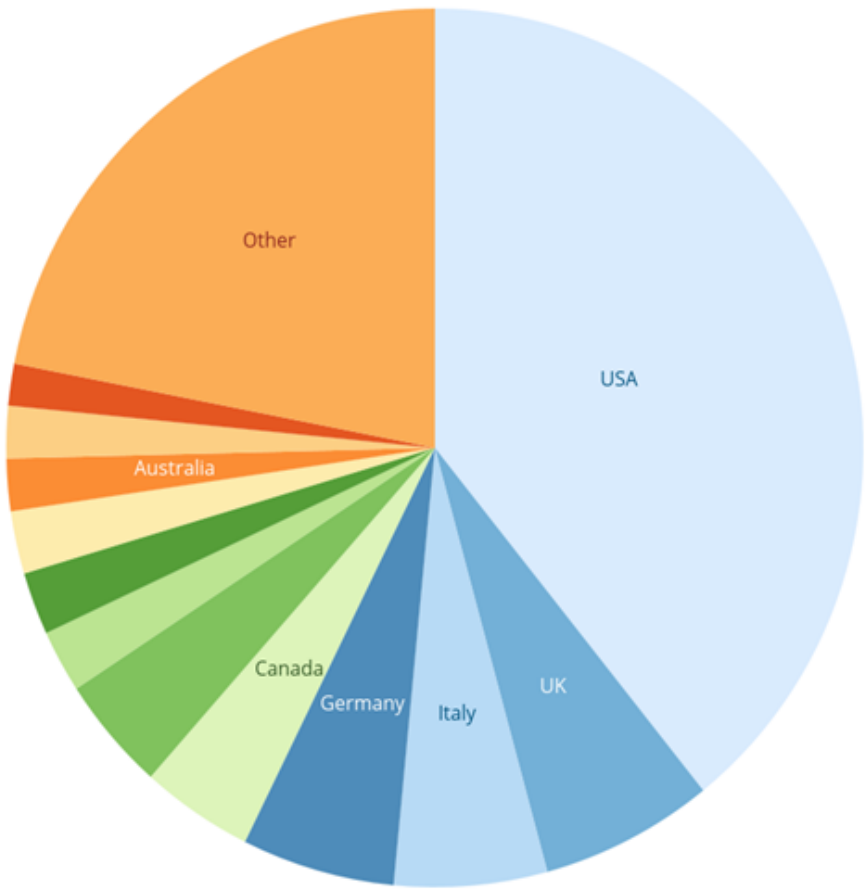
The March data was consistent with the first two months of the year, and the most active ransomware gangs during this month continued to be LockBit, followed by Conti, with an increase in BlackCat (ALPHV), a suspected rebrand of the DarkSide & BlackMatter ransomware groups.

Ransomware Attacks by Gang

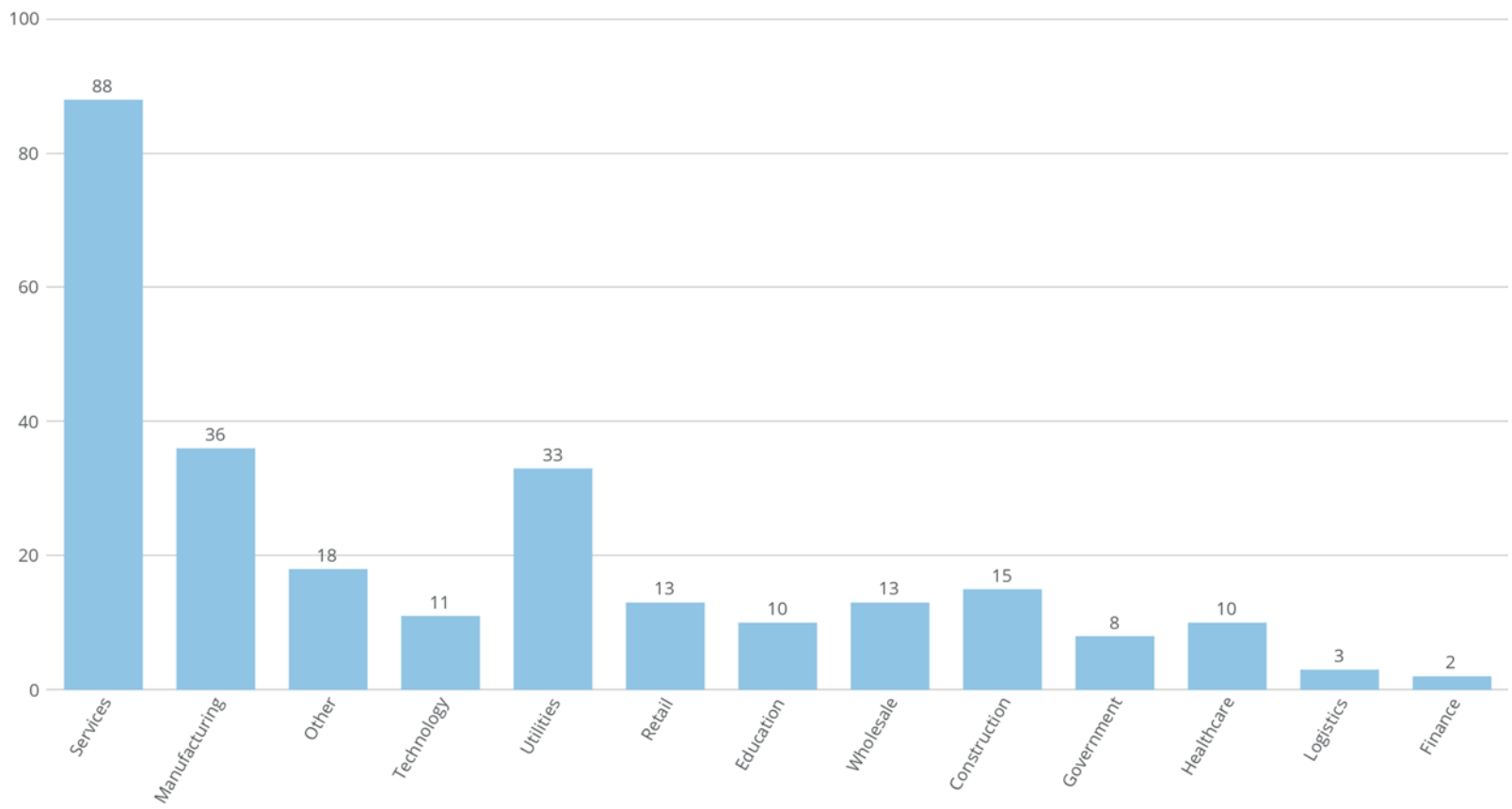


Ransomware Attacks by Country

USA	102	39.2%
UK	17.0	6.54%
Italy	15.0	5.77%
Germany	15.0	5.77%
Canada	11.0	4.23%
Switzerland	11.0	4.23%
Spain	6.00	2.31%
France	6.00	2.31%
Argentina	6.00	2.31%
Australia	5.00	1.92%
Hong Kong	5.00	1.92%
Sweden	4.00	1.54%
Other	57.0	21.9%



Ransomware Attacks by Industry



Ransomware Mitigations

Source: IC3.gov

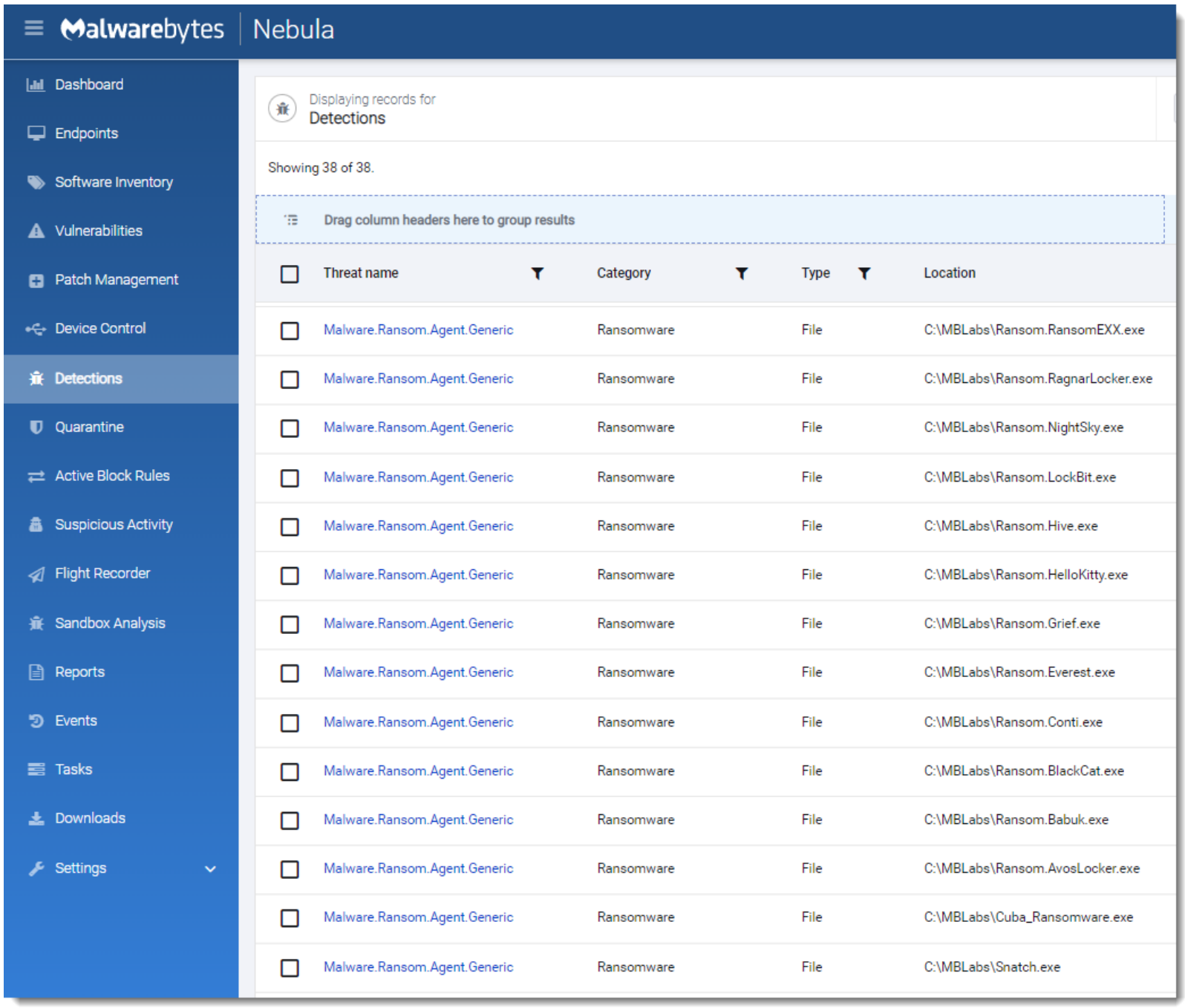
- Implement regular backups of all data to be stored as air-gapped, password-protected copies offline. Ensure these copies are not accessible for modification or deletion from any system where the original data resides.
- Implement network segmentation, such that all machines on your network are not accessible from every other machine.
- Install and regularly update antivirus software on all hosts, and enable real-time detection.
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Audit user accounts with administrative privileges and configures access controls with the least privilege in mind. Do not give all users administrative privileges.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs for any unusual activity.
- Consider adding an email banner to emails received from outside your organization.

- Disable hyperlinks in received emails.
- Use double authentication when logging into accounts or services.
- Ensure routine auditing is conducted for all accounts.
- Ensure all the identified IOCs are input into the network SIEM for continuous monitoring and alerts.

How Malwarebytes protects against ransomware

Malwarebytes can protect systems against all ransomware variants in several ways.

The Malwarebytes Anti-Malware technology detects malicious files, browser modifications, and system modifications on Windows PCs using a combination of signature-based and signatureless technologies. This layer of protection detects the Ransomware binary itself. Detections can happen in real-time as the binary is run or the infection can be rooted out from an already-compromised machine by conducting a full system scan.



Anti-Ransomware is a signatureless technology in charge of monitoring system activity of processes against a certain subset of data in specific locations on the endpoint. Using patented technology, Anti-Ransomware assesses changes in those data files. If an internal scoring threshold is crossed by a monitored process, it triggers a detection from the Anti-Ransomware component.

For those already infected, Ransomware Rollback can help recover encrypted files within 72 hours of the attack. Rollback creates a local cache on the endpoint to store changes to files on the system. It can use this cache to help revert changes caused by a threat. The Rollback feature is dependent on activity monitoring available in Malwarebytes Endpoint Detection and Response.

SHARE THIS ARTICLE

ABOUT THE AUTHOR

Threat Intelligence Team