KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Ruthless QBot Campaign and BlackBasta Ransomware targets victims worldwide

Tracker ID: TN1125 **Date:** 25/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

Background

In a recent investigation of a potentially widespread ransomware campaign, multiple infections of BlackBasta using QBot were observed at the beginning of November 2022, which is actively targeting victims' environment worldwide. These QBot infections started with spam or phishing emails that contained malicious URL links. BlackBasta's principal strategy for maintaining a presence on victims' networks was QBot.

The ransomware group that first appeared in April 2022 and targeted businesses in the United States, Canada, the United Kingdom, Australia, and New Zealand. The group is well-known for adopting double-extortion tactics, in which they steal sensitive files and information from victims and then threaten to publish the data unless the victim pays the ransom. The BlackBasta ransomware gang has been detected in recent campaigns using the QBot malware to create an initial point of entry and move laterally within an organization's network.

QBot, also known as QakBot or Pinkslipbot, is a banking trojan that primarily steals financial information from victims, such as browser information, keystrokes, and credentials. It is a Windows-based malware that began as a banking Trojan and evolved to become a malware dropper. It is employed by numerous ransomware groups to gain access to corporate networks. Phishing is commonly used to commence the QBot deployment process via malicious email attachments and similar lures. After successfully infecting an environment, QBot installs a backdoor, allowing the threat actor to drop further malware, specifically ransomware.

One such attack began with a QBot infection, which led to the loading of Cobalt Strike on many important machines, eventually leading to the global deployment of BlackBasta ransomware. To make recovery even more difficult, the threat actor additionally locked the victim out of the network by disconnecting DNS services, which was a typical approach used on multiple victims. During the compromise, the threat actor was also seen employing Cobalt Strike to get remote access to the domain controller. Finally, it disabled security systems like EDR and antivirus software and installed ransomware.

QBot used different vectors to transmit an ISO or IMG file (disk image file, like the ISO format) via phishing for the initial compromise. It was also discovered using a zero-day MOTW (Mark of the Web) vulnerability to send malicious image (ISO or IMG) files before Microsoft published a patch. "Mark of the Web," a feature that allows Windows to flag a file with metadata such as the download URL and alerts users before opening it. After the latest patch fixed the flaw, threat actor moved on to another zero-day for MOTW, which allows them to bypass Microsoft security flags by embedding a malformed signature inside malicious files. QBot also switched from JavaScript to VBS for loading its harmful payload.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Ruthless QBot Campaign and BlackBasta Ransomware targets victims worldwide

Tracker ID: TN1125 **Date:** 25/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

Furthermore, according to recent research, the threat actor who developed the impairment tool used by BlackBasta is likely the same operator who has access to the packer source code used in FIN7 activities, demonstrating for the first time a plausible link between the two groups. This spike in QBot activity and widespread BlackBasta campaign shows the threat actor's continuous capability evolution to improve the targeting and compromise of several victims. Therefore, we request organizations stay vigilant, protect and prioritize patching of critical assets to proactively identify the threat actor before they infiltrates.

MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion, Command and Control and Data Exfiltration.

Indicators of Compromise

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Prioritize patching of any existing vulnerabilities and harden the applications and infrastructure.
- Ensure that patches for actively exploited vulnerabilities such as ZeroLogon, NoPac, and PrintNightmare for local and domain privilege escalation are deployed.
- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Verify the email sender and content before downloading attachments or selecting embedded links from emails. Hover the pointer above embedded links to show the link's target.
- Enforce periodic password changes and key rotation for critical assets and remote access services [VPN and RDP]. Make sure the credentials are complex, unique, and not reused on another platform.
- Consider enabling multi-factor authentication, especially for public facing services/remote access applications.
- Lookout for any suspicious activities via following Windows Binaries CMD.exe, PowerShell, Task Scheduler, WinRm, WMI/WMIC and Rundll32.
- Identify and block malicious PowerShell activities that query information against Active Directory Domain Services with the "System.DirectoryServices.DirectorySearcher class".
- As a protective measure, prevent unnecessary PowerShell execution by implementing policies and standards that permit only signed scripts to execute.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Ruthless QBot Campaign and BlackBasta Ransomware targets victims worldwide

Tracker ID: TN1125 **Date:** 25/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

- Consider disabling auto-mounting of disc image files (primarily .iso, .img, .vhd, and .vhdx) globally via GPOs to prevent such an infection technique from succeeding. This can be accomplished by altering the registry values associated with Windows Explorer file associations to prevent the Explorer's automatic "Mount and Burn" popup for these file extensions. (This does not disable the mount functionality.)
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Deploy appropriate security controls such as latest AV/EDR, Firewall, IDS for monitoring and mitigating the cyber threats.
- Implement proper network segmentation with controlled access to services and applications and disable unnecessary services and ports.
- Establish a data recovery strategy and routinely backup your files to a secure offsite location, where the ability to rescue your data after a ransomware assault is guaranteed by routine data backups.

References

- THREAT ALERT: Aggressive Qakbot Campaign and the Black Basta Ransomware Group Targeting U.S. Companies, Cybereason Global SOC Team, 23rd November 2022, External Link (www.cybereason.com).
- Noah Campbell, Threat Actors Leverage Windows Zero-Day Vulnerability to Deploy QBot Malware, BlackBerry, 22nd November 2022, External Link (blogs.blackberry.com).
- Antonio Cocomazzi and Antonio Pirozzi, CRIMEWARE, Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor, Sentinel LABS, 03rd November 2022, External Link (www.sentinelone.com).
- Bill Toulas, Black Basta ransomware gang linked to the FIN7 hacking group, Bleeping Computer, 03rd November 2022, External Link (www.bleepingcomputer.com).

KPMG in India Cyber Response Hotline : +91 9176471471

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.