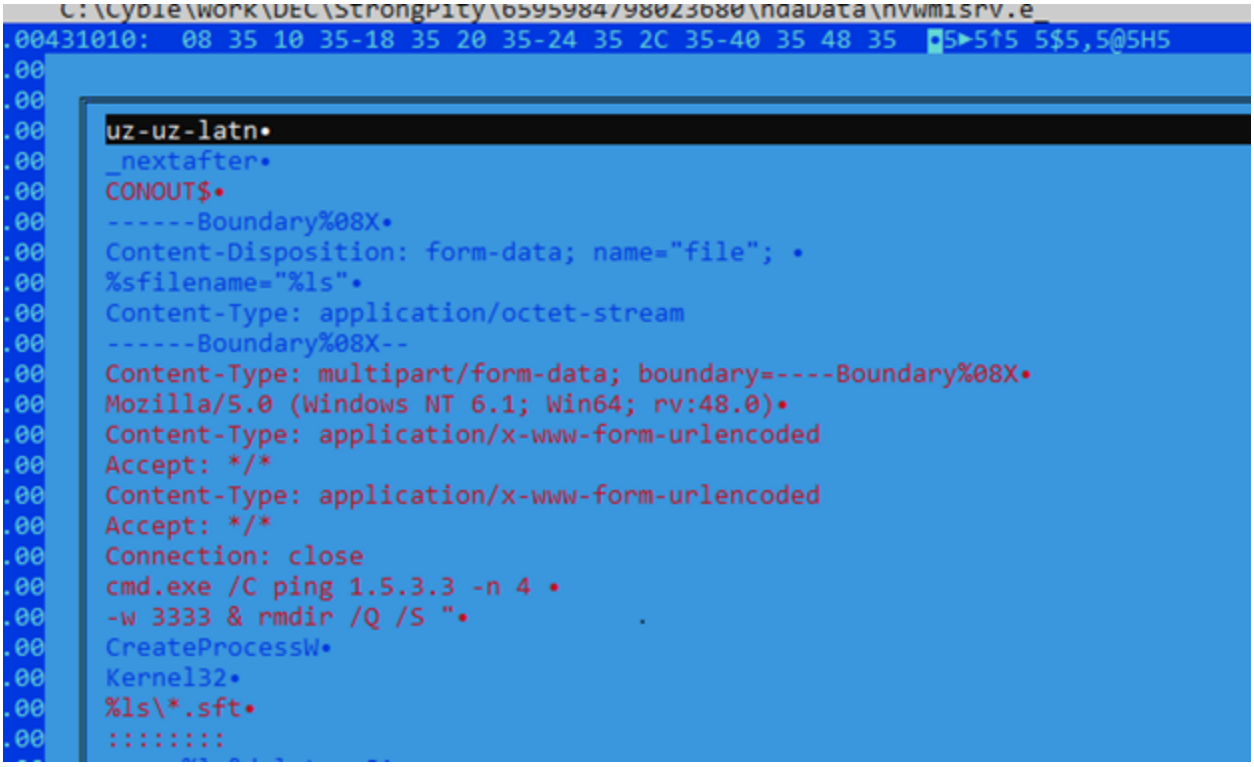
StrongPity APT Extends Global Reach with New Infrastructure

cybleinc.com/2020/12/31/strongpity-apt-extends-global-reach-with-new-infrastructure/

December 30, 2020



StrongPity/Promethium APT, also known as APT-C-41, has been active since at least 2012. It was first publicly reported in October 2016, after cyberattacks against users in Belgium and Italy in which it used the watering-hole attack technique to deliver malicious versions of WinRAR and the TrueCrypt file encryption software.

The group chiefly uses Truvasys, a first-stage malware that has been employed in several attack campaigns with trojanized common computer utilities, including WinRAR, WinUtils, TrueCrypt, or SanDisk. In each of its campaigns, the Truvasys malware has emerged with evolved features.

Researchers described StrongPity as having the distinctive features of an APT unit that utilizes zero-day vulnerabilities and sophisticated attack tools to invade victims for espionage. After the 2016 attack, the threat actor has expanded its TTPs to include watering hole attacks and mass phishing email campaigns.

Here is the timeline of StrongPity APT group starting from 2016.

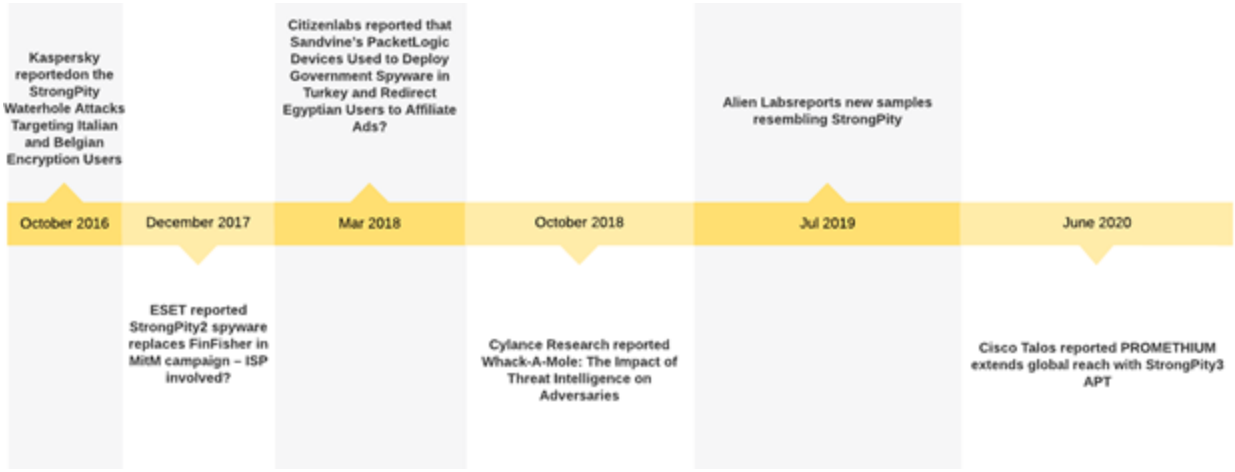


Figure 1. Timeline of the StrongPity APT attacks

In 2016, APT-C-41 was mostly targeting countries like Italy and Belgium. However, its victims are now widespread across Europe, Northern Africa, Canada, and Asia. Focused on finding and exfiltrating data from infected machines, the StrongPity APT group runs a series of counterfeit websites that pretend to offer an array of software tools. These utilities provide trojanized versions of legitimate applications.

While tracking the StrongPity APT group's campaigns, we discovered that it targets through Trojanized Partition Find and Mount software utility along with updated C&C infrastructure. In this blog, we have highlighted the technical details of the latest cyberattacks by the group.

The high-level process flow of the StrongPity malware installation is shown in the figure below.

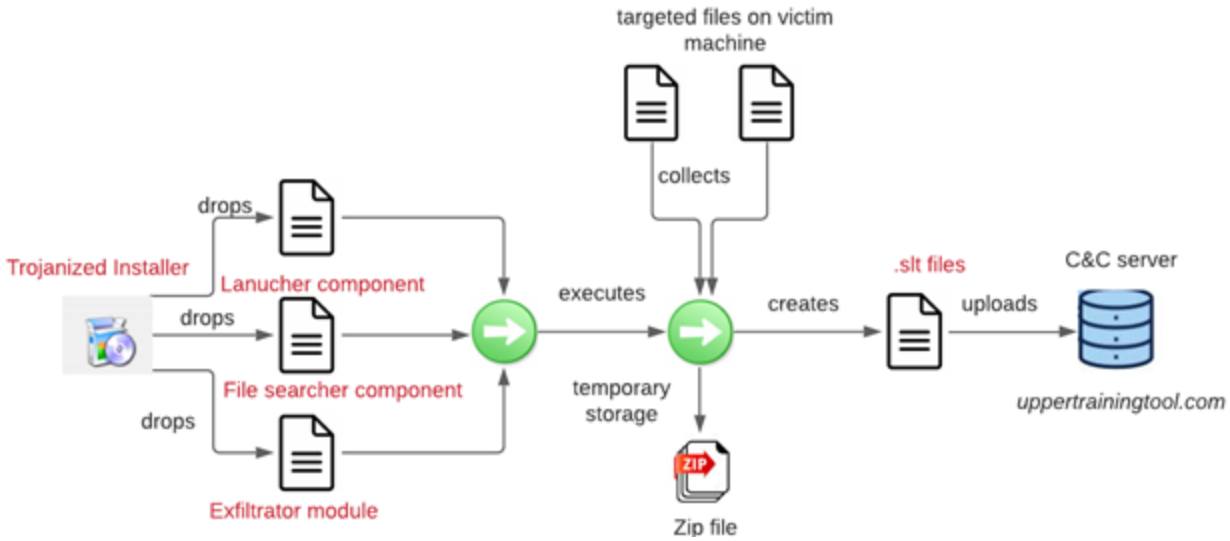


Figure 2: High-level execution flow diagram

The high-level execution flow of the StrongPity infection is as follows:

- It starts with the APT actor employing the watering hole attack or Phishing email to deliver trojanized Partition Find and Mount software utility on the victims.
- The Trojanized installer drops multiple malware components in the %temp%\ndaData folder along with configuration files, as shown below.

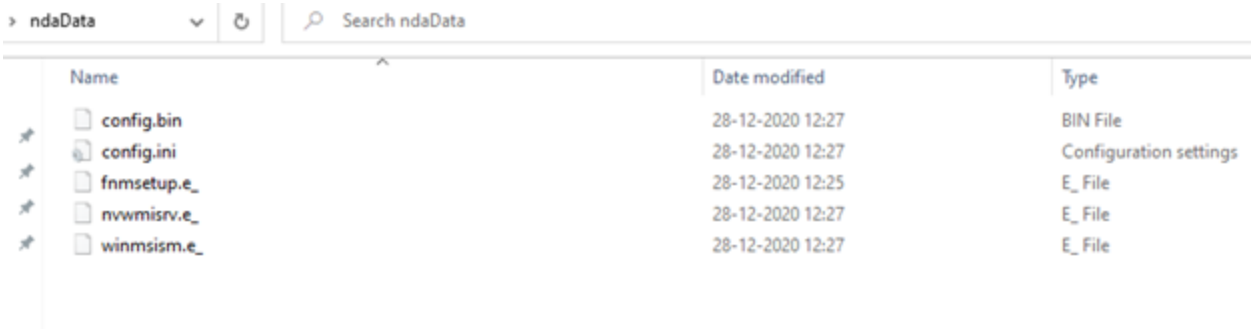


Figure 3: Dropped payload files and config files

- The Launcher component is responsible for executing the Exfiltrate module, which runs another File searcher component.
- The File searcher component enumerates system drives and looks for target files with specific extensions. The list of extensions is embedded in the StrongPity payload.
- If the files are found in the victim's machine, it will be copied into a temporary zip archive. After completion of adding the files to the archive, it splits into hidden .sft encrypted files.
- These hidden .sft files are sent to the C&C server through a POST request and are then removed from the disk-based on further C&C command. The Exfiltrate module has commands to delete the .sft files after being sent to the hacker C&C server, as seen in the figure below.

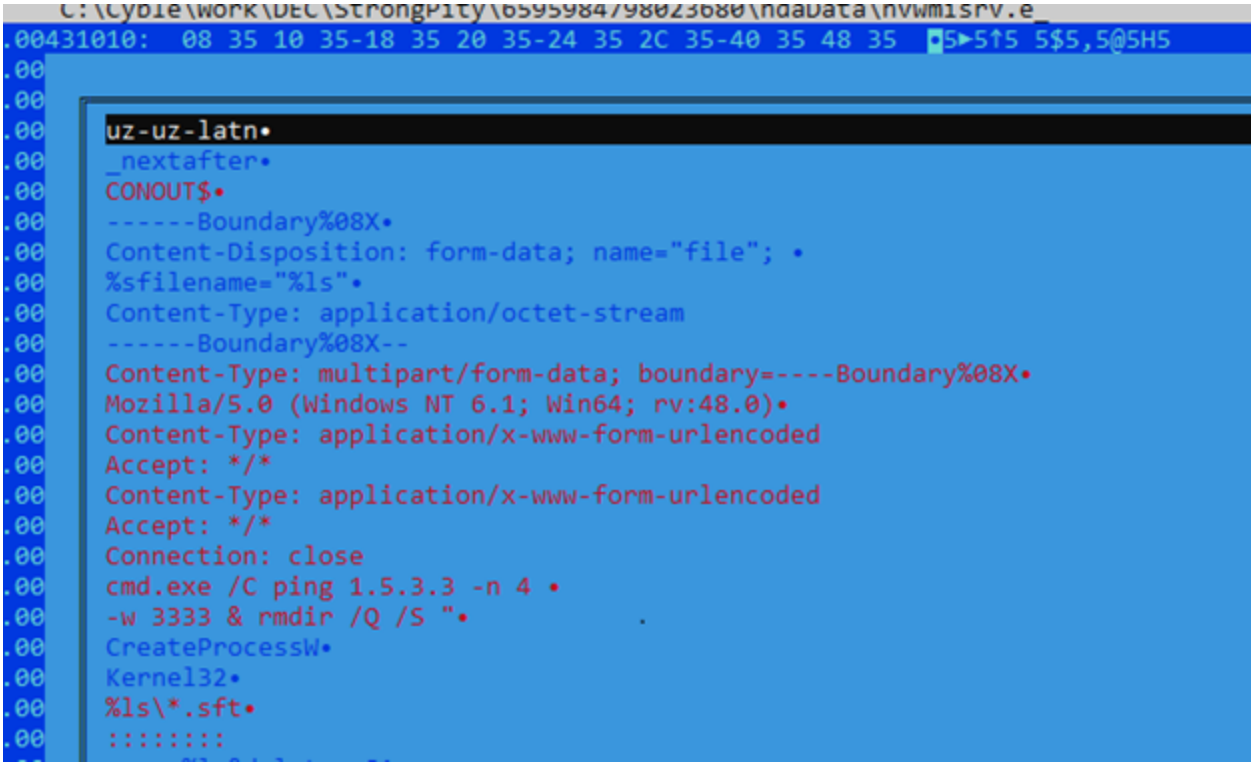


Figure 4: Payload module with the deletion command

Upon execution of the trojanized installer, it extracts and drops encrypted payloads, which is part of its resource section, as shown in the figure below

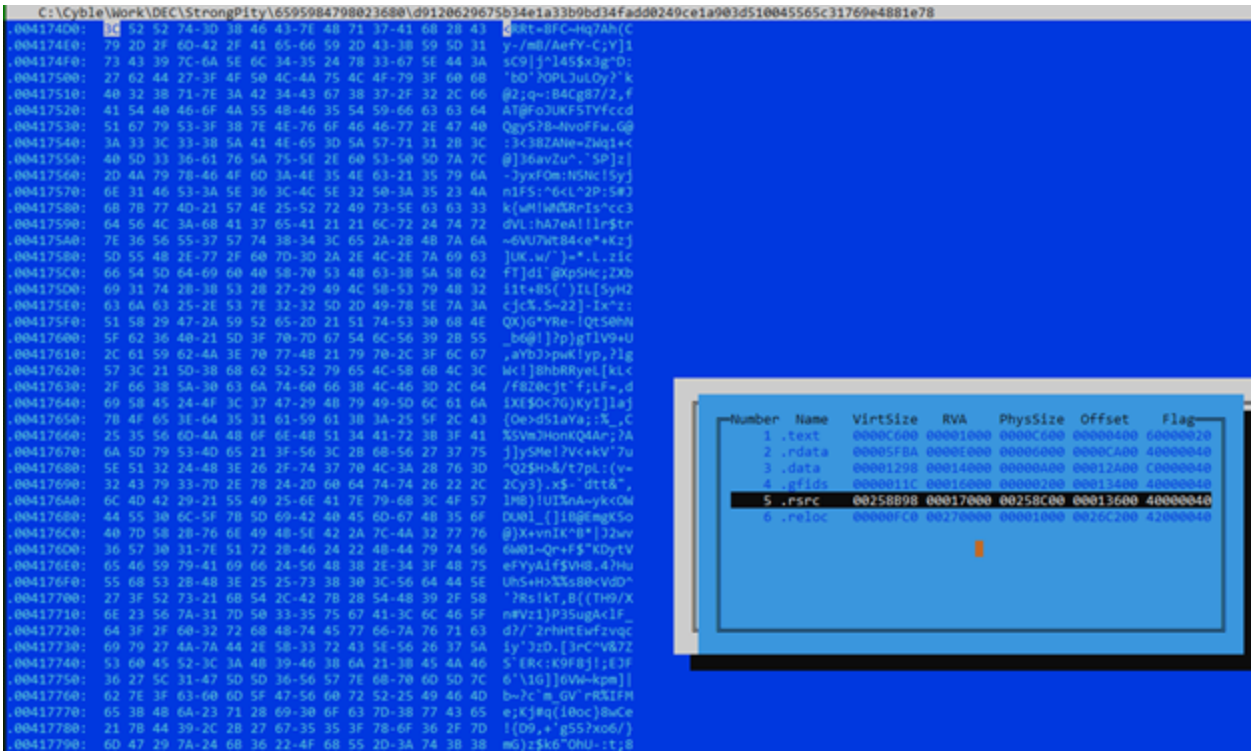


Figure 5: Encrypted payload in .rsrc section

StrongPity payloads such as the Launcher & Persistence component, Exfiltration & Command Execution module, and the File Searcher component are extracted and dropped in the %temp%\ndaData folder. The figure below shows the decryption routines as well as decrypted payloads in the process memory.

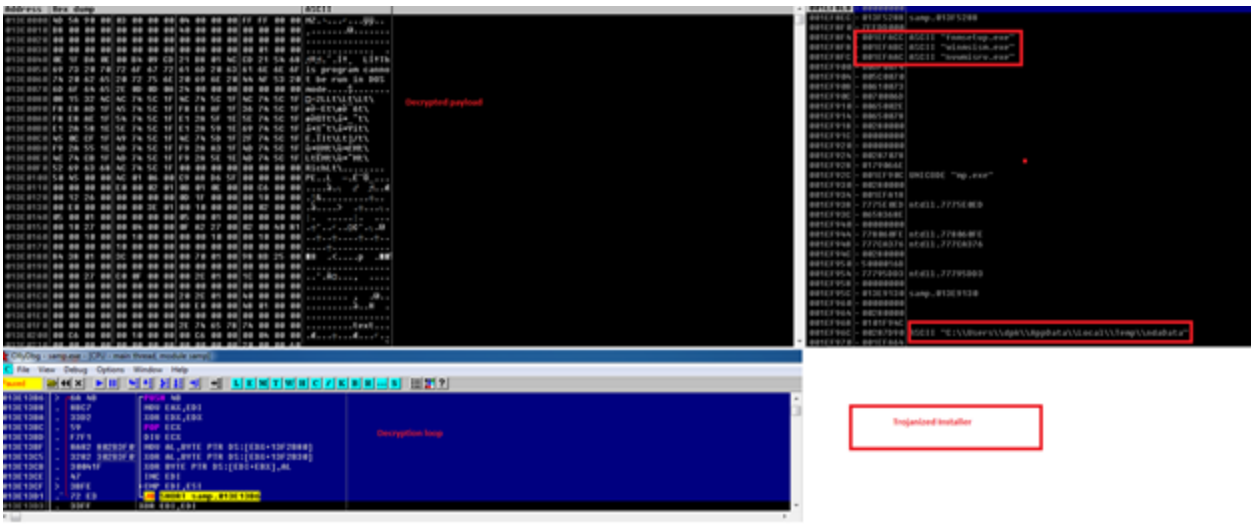


Figure 6: Decrypted payload in the memory

The malware payload creates a mutex named “thUseiGpkMkPkFYrIOvKN” to mark its existence on the victim’s system, as shown in the image below.

Figure 7: Creates Mutex function in the payload file

The Exfiltrate component has a hardcoded C&C URL, decoded in the memory as depicted in the debugger image below. As seen in earlier variants, the Parse_ini_file.php is used as part of the layer 1 communication and the functionality to get commands from the C&C server.

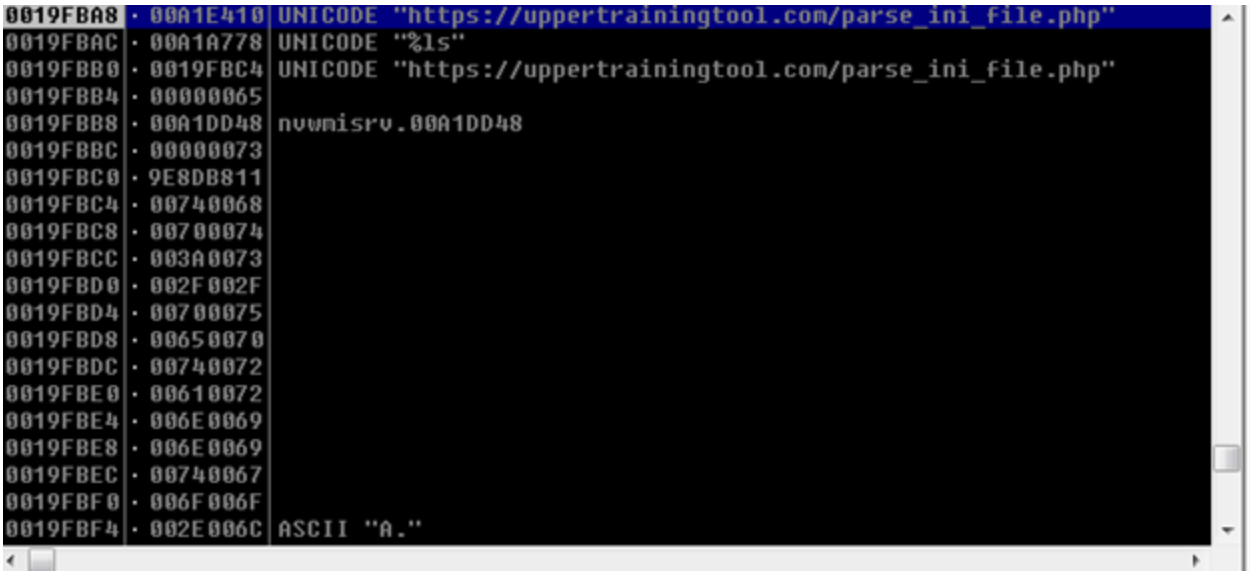


Figure 8: Layer1 C&C link in payload file

The network capture depicts multiple connection requests to the attacker layer 1 C&C server (uppertrainingtool[.]com) as showcased in the Wireshark image below.

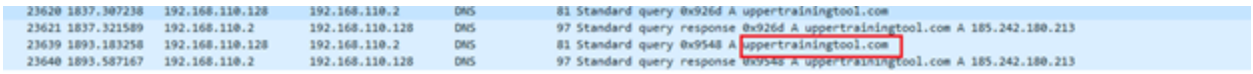


Figure 9: Wireshark image of C&C communication

Conclusion:

The StrongPity APT group has suspected ties to state-sponsored campaigns and has the ability to search and exfiltrate multiple files or documents from the victim's machine. This group uses a 3-layer C&C for thwarting forensic investigations and operates with fully functional Trojanized popular tools.

The Cyble Research team is continuously monitoring to harvest the threat indicators/TTPs of emerging APTs in the wild to ensure that targeted organizations are well informed and proactively protected.

MITRE ATT&CK Framework:

ID	Description	Use
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Used Registry run keys to establish persistence.
T1543.003	Create or Modify System Process: Windows Service	Created new services and modified existing services for persistence.
T1587.003	Develop Capabilities: Digital Certificates	Created self-signed digital certificates for use in HTTPS C2 traffic.
T1189	Drive-by Compromise	Used watering hole attacks to deliver malicious versions of legitimate installers.
T1036.005	Masquerading: Match Legitimate Name or Location	Disguised malicious installer files by bundling them with legitimate software installers.
T1204.002	User Execution: Malicious File	Tried to get users to execute compromised installation files for legitimate software including compression applications, security software, browsers, file recovery applications, and other tools and utilities.
T1036.004	Masquerade Task or Service	Named services to appear legitimate.

Source: https://attack.mitre.org/groups/G0056/

Indicators of Compromise (IOC's):

File hashes:

– 469C0460E4C1FEFD01DB4AE9F79C53C7
– 81390CE601D34F384BFF9198EEF793A9
– 8C24DD49D037121212985C722E1C7D03
– A969A009D0927B1B4D9F8BB3C1CA49BE
– C81DCDD13572C151B6E04AA4D8A6DD43

C2 Domains:
– uppertrainingtool[.]com
– updserv-east-cdn3[.]com
– hybirdcloudreportingsoftware[.]com
– transferprotocolpolicy[.]com

About Cyble

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the darkweb. Cyble's prime focus is to provide organizations with real-time visibility into their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Startups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.io.