PERISCOPE

March 2, 2022

INTEL471

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **f41r3r79x0r**, **FAJET**, **islianan** and **ISLIX** offered exploits and the actors **ErraticGalia**, **heart43** and **Mr.DDoS** offered distributed denial-of-service (DDoS) utilities. Additionally, the actors **demWTF**, **mont4na**, **Red_Goddess1** and the Everest ransomware-as-a-service (RaaS) operator or operators targeted the energy, resources and agriculture sector, while the actor **Carzita** and the Civilian RaaS operator or operators targeted websites of Ukrainian government, military and financial institutions.

Threat actors offer exploits

- On Feb. 19, 2022, the actor **f41r3r79x0r** advertised a fully undetectable (FUD) malicious document (maldoc) with a built-in macro. The actor also offered to provide a maldoc to exploit the Microsoft MSHTML remote code execution (RCE) vulnerability CVE-2021-40444 with the option to include a macro, but stated the maldoc was detected by some antivirus software except Windows Defender.
- On Feb. 20, 2022, the actor **islianan** advertised a marketplace allegedly selling exploits for zero-day vulnerabilities. The actor also offered others to sell their exploits on the marketplace and shared links to its websites.
- On Feb. 20, 2022, the actor **ISLIX** offered exploit development services. The actor allegedly would take orders for the development of silent Microsoft Word ([.]doc) exploits that would be FUD by antivirus software and would bypass Gmail protections.
- On Feb. 23, 2022, the actor **FAJET** offered to sell an exploit kit that allegedly leveraged zero-day vulnerabilities, included more than 30 private exploits and was designed to spread malware automatically. The description claimed the exploited browser would run shellcode and download a keylogger trojan file from a command and control (C2) server to be unpacked and installed in the infected machine later. The malware allegedly could steal cookies, user sessions and login credentials, had an automated crypting feature and was FUD.

Threat actors offer distributed denial-of-service utilities

- On Feb. 18, 2022, the actor **ErraticGalia** advertised a DDoS botnet dubbed Galia. The botnet allegedly could be used to launch Open Systems Interconnection (OSI) model Transport Layer 4 and other types of DDoS attacks and each attack had power ranging from 50 Gigabits per second (Gbps) to 100 Gbps. The description claimed the botnet also could bypass multiple anti-DDoS protection solutions.
- On Feb. 19, 2022, the actor **Mr.DDoS** offered multilevel DDoS attacks aimed to destroy rivals. A private hosting service and more than 1,000 servers allegedly allowed the actor to compete with the leading market players using an allegedly unique method to overload the target. This special technique allegedly eliminated defense mechanisms instead of bypassing them. The actor allegedly could take down commerce and gaming resources and government websites at flexible prices.
- On Feb. 21, 2022, the actor **heart43** offered a service to conduct DDoS attacks on OSI model Application Layer 7. The actor claimed DDoS protection from ArvanCloud, Cloudflare, DDoS-GUARD, OVH and Project Shield could be bypassed. Multiple attack methods allegedly could be used, including GET, hypertext transfer protocol (HTTP) and POST flood attacks.

Threat actors target energy, resources, agriculture sector

- On Feb. 19, 2022, the Everest RaaS operator or operators offered to sell access to several networks. The first allegedly was access with root privileges to Linux-based servers of an undisclosed state-owned company that generated, transmitted and distributed electricity. The operator or operators also claimed the country's largest defense electronic equipment company appeared in the files and accesses. The other accesses were to undisclosed networks on the [.]gov and [.]edu domains in Argentina, France, the U.K. and the U.S.
- On Feb. 19, 2022, the actor **Red_Goddess1** offered to sell unauthorized access to Brazilian military and defense entities. The description claimed one access was gained via compromised Citrix account credentials and the other was domain-level access to a Windows-based endpoint.
- On Feb. 20, 2022, the actor **demWTF** offered unauthorized access to an undisclosed Spain-based energy company allegedly in the top 300 companies of the world with a US $35 billion revenue. The actor claimed to have access to user information, invoices and more via compromised F5 accounts.
- On Feb. 21, 2022, the actor **mont4na** offered to sell login credentials allegedly stolen from a U.S.-based gas and electric utility holding company. The actor claimed the data leak impacted more than 10,000 user email accounts, 10 administrator accounts, 10 employee user accounts and one email service user account. The actor also offered to provide the vulnerability used to extract the data.

Threat actors target websites of Ukrainian government, military, financial institutions

- On Feb. 19, 2022, the actor **Carzita** threatened to "order a few dedicated servers to launch attacks against Ukrainian websites" apparently referring to DoS attacks with a focus on banks, government portals and military resources. The attacks allegedly would start Feb. 22, 2022, and last for at least a week. The actor also threatened to deface any [.]ua domains and provided a link to an alleged archive with data from the hacked websites.
- On Feb. 24, 2022, the Civilian RaaS operator or operators claimed several data leaks that impacted multiple entities in Ukraine. The operators claimed corporate email access to the Ministry of Communities and Territories Development with official correspondence of department employees. The leak allegedly also included information about diseases, diagnoses and doctors of employees of the Ministry of Internal Affairs and scanned copies of passports and driver's licenses of citizens of Ukraine as well as some commercial documents. Other targets allegedly included Kyiv city portals.