PERISCOPE

March 23, 2022

INTEL471

TLP: AMBER

WEEKLY UNDERGROUND UPDATE

Last week in the underground, the actors **ArokkhGof**, **bitcoin.btc** and **SpaceX_Drop** offered drop accounts and money mule services and the actors **afron** and **isli** offered malware that bypassed Windows Defender antivirus protection. Additionally, the actors **Foxpro** and **LongPig** compromised Signaling System 7 (SS7) gateways; the actors **Ellnoir**, **inthematrix**, **Saprano** and the Avos ransomware-as-a-service (RaaS) operator or operators targeted the energy, resources and agriculture sector; and the actors **shazze** and **ZironTool** offered malware crypting services and tools.

Threat actors offer drop accounts, money mule services

- On March 11, 2022, the actor **bitcoin.btc** sought partners with traffic. The actor claimed to have a bank phishing page and insiders who allegedly could provide drop accounts, remove transfer limits from accounts and mute notifications sent to victims to withdraw funds from accounts instantly. Cashout services allegedly could be provided the same day money transfers were received if within banking hours.
- On March 15, 2022, the actor **SpaceX_Drop** advertised a cashout and money mule service with payment cards for several banks available. The actor offered to sell the cards or provide them for cashout purposes in addition to providing access to online banking accounts for a cut of profits from money transfers.
- On March 16, 2022, the actor **ArokkhGof** offered to sell debit cards registered by money mules. The cards allegedly only were available to order, came with a 30-day warranty and could be delivered internationally. The actor claimed more than 300 fully controlled mules were available in 27 countries with new mules recruited as necessary.

Threat actors offer malware bypassing windows defender

- On March 12, 2022, the actor **afron** offered to rent out a nonresident loader designed to be spread via landing pages. The malware allegedly could bypass Windows Defender and protection mechanisms from Google Chrome and Microsoft SmartScreen, was compatible with Windows 10 to 11 operating system versions and supported the Microsoft Installer (MSI) file format. The actor also claimed a bot with hidden virtual network computing (HVNC) functionality was under development and interested customers were offered to test it.
- On March 14, 2022, the actor **isli** advertised cryptomining malware dubbed sYMiner. The actor claimed the miner could mine 10 cryptocurrencies, was fully undetectable (FUD), could bypass Windows Defender and spread via USB drives and local area networks (LANs).

Threat actors compromise Signaling System 7 gateways

- On March 11, 2022, the actor **Foxpro** offered to sell access to an undisclosed internet service provider (ISP) and SS7 gateways in Asia. The actor allegedly would provide AnyDesk passwords, gateway passwords, IP address ranges and remote desktop protocol (RDP) access credentials.

- On March 14, 2022, the actor **LongPig** offered to sell information about a zero-day remote code execution (RCE) vulnerability that allegedly impacted the web panel of the NetBorder SS7 gateway. The actor claimed the vulnerability could be leveraged to obtain root access and execute virtually any bash commands without requiring login credentials. The actor also promised to provide an obfuscated bash script to create a reverse shell connection via the Netcat networking utility.

Threat actors target energy, resources, agriculture sector

- On March 11, 2022, the actor **Saprano** offered to sell unauthorized access with domain administrator privileges via compromised RDP and virtual private network (VPN) account credentials to an undisclosed Austria-based water and power supplier and electric power producer. The description claimed the entity had a revenue of 17 million according to ZoomInfo or 36 million according to Dun & Bradstreet in an unspecified currency. The actor allegedly conducted scanning with the NetScan utility, which showed 25 devices on the network.
- On March 12, 2022, the actor **Ellnoir** offered to sell unauthorized access with local administrator privileges via compromised RDP account credentials to an undisclosed Europe-based oil and gas company. The description claimed the victim had more than US $10 billion in revenue, operated in more than 20 countries and had about 15,000 hosts on the network. The actor claimed access to the network was gained via a compromised F5 account and the compromised machine was not in the domain.
- On March 16, 2022, the Avos RaaS operator or operators claimed to compromise a Canada-based renewable energy company. The threat actors allegedly exfiltrated the company's files and shared some documents as proof of the claim. They also threatened to publish the full data leak if the victim company refused to negotiate.
- On March 16, 2022, the actor **inthematrix** offered to sell unauthorized access via RDP account credentials to an undisclosed European naval shipping company with an alleged annual revenue of US $30 million. Local administrator privileges allegedly allowed partial access to the network with 120 devices. The actor claimed the buyer would be able to access a mail server with more than 1 TB of data and advised the future buyer to infect the company with ransomware.

Threat actors offer malware crypting services, tools

- On March 12, 2022, the actor **shazze** offered file crypting services to enable malware to evade detection by antivirus tools. The actor allegedly could crypt any malicious files, effectively bypassing Google Chrome defense mechanisms and ensuring a good hit rate. Customers allegedly could choose between shared and unique stub files and have files recrypted for free if initial crypting resulted in a certain amount of detection alerts.
- On March 15, 2022, the actor **ZironTool** offered to rent out a crypting tool of the same name. The tool allegedly was written in the Assembly and C# programming languages and allowed bypassing Avast sandbox and memory scan features, disabling services and showing fake message boxes, among other things. The description claimed the actor's team worked on crypters since 2009, offered private and public stubs updated every week or instantly after they were detected and guaranteed low runtime and scantime detection rates.