Escanor Malware delivered in Weaponized Microsoft Office Documents

resecurity.com/blog/article/escanor-malware-delivered-in-weaponized-microsoft-office-documents

Back

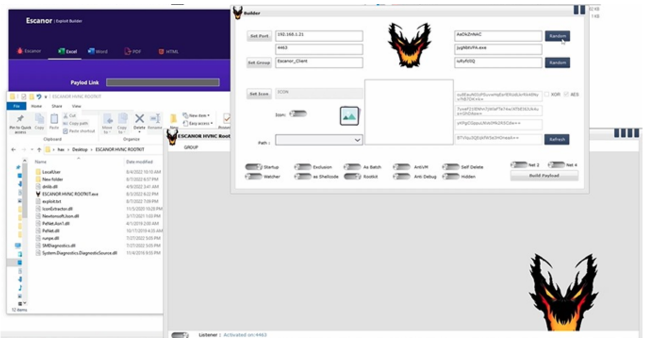
Cybercrime Intelligence

21 Aug 2022

cybercrime, malware, RAT, Dark Web, Android

Resecurity, a Los Angeles-based cybersecurity company protecting Fortune 500 worldwide, identified a new RAT (Remote Administration Tool) advertised in Dark Web and Telegram called Escanor. The threat actors offer Android-based and PC-based versions of RAT, along with HVNC module and exploit builder to weaponize Microsoft Office and Adobe PDF documents to deliver malicious code.

The tool has been released for sale on January 26th this year initially as a compact HVNC implant allowing to set up a silent remote connection to the victim's computer, and later transformed into a full-scale commercial RAT with a rich feature-set. Escanor has built a credible reputation in Dark Web, and attracted over 28,000 subscribers on the Telegram channel. In the past, the actor with the exact same moniker released 'cracked' versions of other Dark Web tools, including Venom RAT, and Pandora HVNC which were likely used to enrich further functionality of Escanor.



Set Port: 192.168.1.21 / 4463

Set Group: Escanor_Client

AaDkZnNAC

jvgNbfVPA.exe

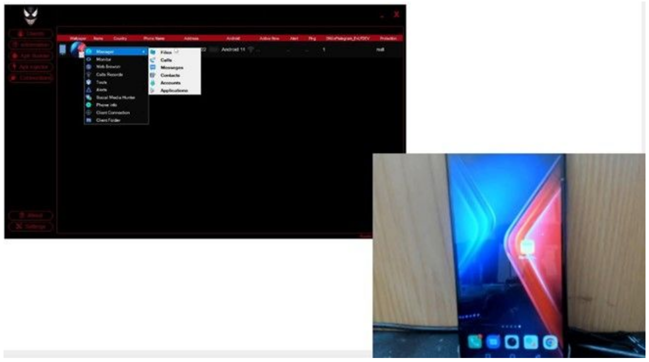
uRyfU0Q

Listener : Activated on:4463

hax › Desktop › ESCANOR HVNC ROOTKIT

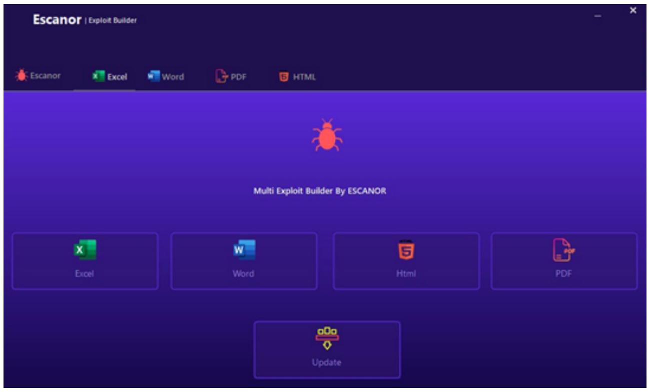
Name	Date modified
LocalUser	8/4/2022 10:10 AM
New folder	8/7/2022 6:57 PM
dnlib.dll	4/9/2022 3:41 AM
ESCANOR HVNC ROOTKIT.exe	8/3/2022 6:22 PM
exploit.txt	8/7/2022 7:09 PM
IconExtractor.dll	11/5/2020 10:28 PM
Newtonsoft.Json.dll	3/17/2021 1:03 PM
PeNet.Asn1.dll	4/1/2019 2:00 AM
PeNet.dll	10/17/2019 4:35 AM
runpe.dll	7/27/2022 5:05 PM
SMDiagnostics.dll	7/27/2022 5:05 PM
System.Diagnostics.DiagnosticSource.dll	11/4/2016 9:55 PM

The mobile version of Escanor (also known as "Esca RAT") is actively used by cybercriminals to attack online-banking customers by interception of OTP codes. The tool can be used to collect GPS coordinates of the victim, monitor keystrokes, activate hidden cameras, and browse files on the remote mobile devices to steal data.

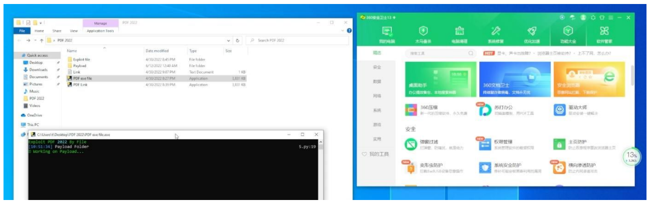


“Fraudsters monitor the location of the victim, and leverage Esca RAT to steal credentials to online-banking platforms and perform unauthorized access to compromised account from the same device and IP – in such case fraud prevention teams are not able to detect it and react timely” – said Ali Saifeldin, a malware analyst with Resecurity, Inc. who investigated several recent online-banking theft cases.

Most samples detected recently were delivered using Escanor Exploit Builder. The actors are using decoy documents imitating invoices and notifications from popular online-services.



Notably, the domain name 'escanor[.]live' has been previously identified in connection to AridViper (APT-C-23 / GnatSpy) infrastructure. APT-C-23 as a group was active within the Middle Eastern region, known to particularly target Israeli military assets. After the report was released by Qihoo 360, the Escanor RAT actor released a video detailing how the tool should be used to bypass AV detection.



C:\Users\t\Desktop\PDF 2022\PDF exe file.exe

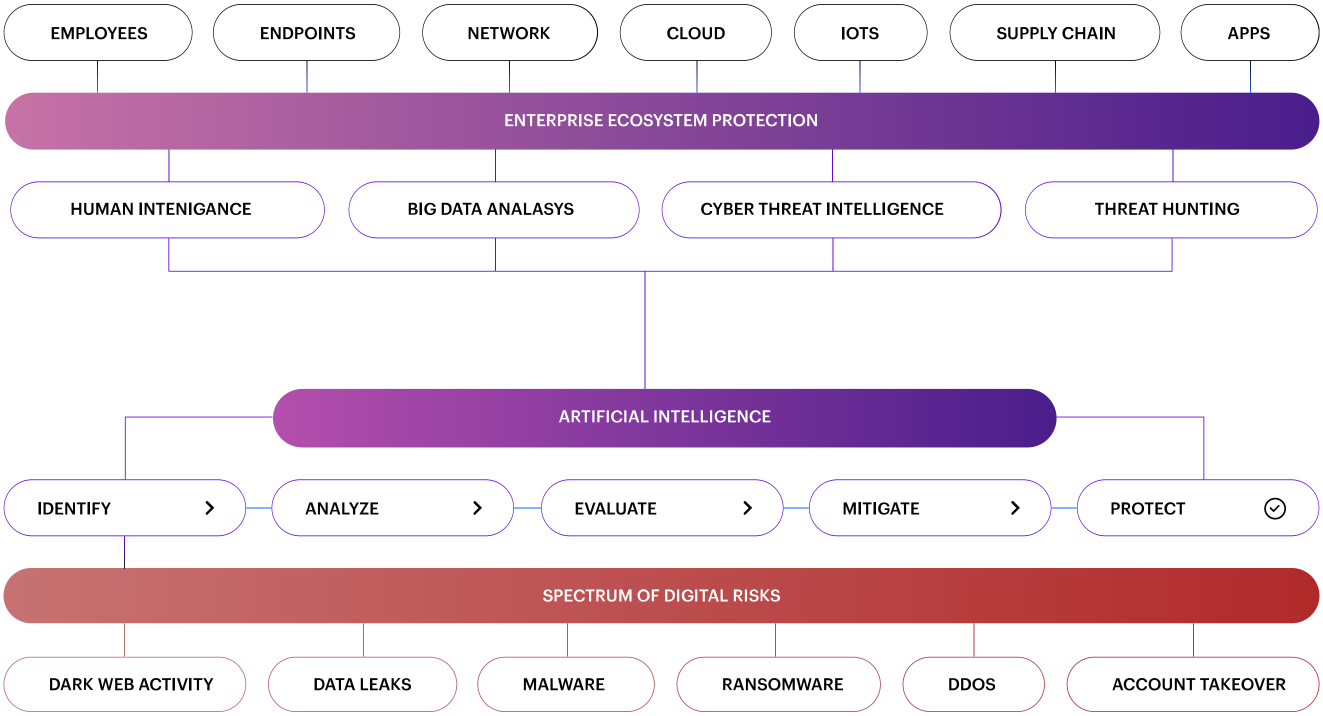
```
Exploit PDF 2022 By File
[10:51:34] Payload Folder                                          5.py:19
: Working on Payload...
```

The majority of victims infected by Escanor have been identified in the U.S., Canada, UAE, Saudi Arabia, Kuwait, Bahrain, Egypt, Israel, Mexico, and Singapore with some infections in South-East Asia.

Reference:

- Mapping out AridViper Infrastructure Using Recon's Malware Module
https://team-cymru.com/blog/2020/12/16/mapping-out-aridviper-infrastructure-using-augurys-malware-addon/

Cloud Architecture



EMPLOYEES ENDPOINTS NETWORK CLOUD IOTS SUPPLY CHAIN APPS

ENTERPRISE ECOSYSTEM PROTECTION

HUMAN INTENIGANCE BIG DATA ANALASYS CYBER THREAT INTELLIGENCE THREAT HUNTING

ARTIFICIAL INTELLIGENCE

IDENTIFY > ANALYZE > EVALUATE > MITIGATE > PROTECT ✓

SPECTRUM OF DIGITAL RISKS

DARK WEB ACTIVITY DATA LEAKS MALWARE RANSOMWARE DDOS ACCOUNT TAKEOVER