

OOTW 11/14/2022

Monday, November 14, 2022 7:48 AM

"Hey everyone, welcome to a another addition to the Out of the Woods Threat Hunting podcast. This is Scott Poley, here with Mike Mitchell and This weekly segment features the top 5 stories that threat hunters need to be thinking about, as well as our thoughts on the subject and hunting strategies.

With that, let's dive into the Top 5 Threat Hunting Headlines for the week of Nov 14th 2022!"

<https://www.itnews.com.au/news/australia-sets-up-100-strong-permanent-operation-to-target-hackers-587691>

ddf

Australia sets up 100-strong permanent 'operation' to target hackers

Hack the Hackers -- stop incidents before they start

- Very cool idea, but so much can go wrong if not governed correctly
- If local in Australia, great --- but like for example Russia supporting groups or protecting groups within their borders --- how is that going to be handled?
- Obviously can't target shared infrastructure for certain things --- cause that is bad
- So best techniques
 - o are collecting intel on people and hope to extradite --- not that successful
 - o Disrupting money making oppurtunities
 - o Possibly disrupting infrastructures in ways that can't impact others --- with out crossing lines with countries laws/regulations

<https://thehackernews.com/2022/11/worok-hackers-abuse-dropbox-api-to.html>

Worok Hackers Abuse Dropbox API to Exfiltrate Data via Backdoor

Hidden in Images

Worok group using PNG files to conceal payloads and collect data and communicate via dropboxAPI

https://decoded.avast.io/martinchlumecky/png-steganography/?utm_source=rss&utm_medium=rss&utm_campaign=png-steganography

Attack Details:

Suspect initial access was ProxyShell

Attack required administrative privileges initially in order to perform the DLL-sideload

- Targeted DLLs
 - WLBSCTRL.DLL (IKEEXT)
 - TSMSISrv.DLL (SessionEnv)
 - TSVIPsrv.DLL (SessionEnv)
- Service relation
 - IKEEXT service (IKE and AuthIP Ipsec Keying Modules)
 - SessionEnv (Remote Desktop Configuration)
- Known for already having DLL files missing --- making it easy to drop own DLL in System32 folder
 - <Look for DLL creation in System32 ; possibly for those DLL names>

Attackers Targeted VMware Machines with DLL-hijacking

- Targeted DLLs
 - vmGuest-Lib.DLL (WMI Performance Adapter) (WmiAPsrv)
- Playing file in the %ProgramFiles% env var directory --- supercedes the original in the System32\Directory

PNG Stego

- Located in the C:\Program Files\Internet Explorer --- fairly inconspicuous
- Uses least significant bit encoding LSB
 - Bit with the least impactful data to the image changed to carry the malicious code when extracted
- XOR encrypted and XOR key is hardcoded in the PNGLoader malware
- Resulting payload is Gzip data

DropBox API

DropBoxControl Method	API
DropBox_FileDownload	https://content.dropboxapi.com/2/files/download
DropBox_DataUpload	https://content.dropboxapi.com/2/files/upload
DropBox_FileDelete	https://api.dropboxapi.com/2/files/delete_v2
DropBox_GetFileList	https://api.dropboxapi.com/2/files/list_folder

Command	Description
cmd	Run cmd /c <param> & exit, the param is sent by the attackers.
exe	Execute a defined executable with specific parameters.
FileUpload	Download data from the DropBox to a victim's machine.
FileDownload	Upload data from a victim's machine to the DropBox.
FileDelete	Delete data from a victim's machine.
FileRename	Rename data from a victim's machine.
FileView	Sent file information (name, size, attributes, access time) about all victim's files in a defined directory
ChangeDir	Set a current directory for the backdoor
Info	Send information about a victim's machine to the DropBox
Config	Update a backdoor configuration file; see Configuration

- DropboxAPI Control File
 - o leproxy.dat
 - Contains the API key

- Interval to check disk
- Up/Down time
- explorer.log contains all actions of the DropBoxControl if sqmapi.dat file exist
 - Contains decrypted data from the ieproxy.dat file

Typical CMDs Run

- rar.exe a -m5 -r -y -ta20210204000000 -hp1qazxcde32ws -v2560k Asia1Dpt-PC-c.rar c:*.doc c:*.docx c:*.xls c:*.xlsx c:*.pdf c:*.ppt c:*.pptx c:*.jpg c:*.txt >nul
- ettercap.exe -Tq -w a.cap -M ARP /192.168.100.99/ //
- <Obviously look for .exe writes to identify tools --- especially in non program file or system directories>

Attribution

- API's tied to Chinese accounts
- Code was poor at best with a lot of duplicate code in multiple places --- signifying not originally developed

<https://thehackernews.com/2022/11/microsoft-blames-russian-hackers-for.html>

Microsoft Blames Russian Hackers for Prestige Ransomware Attacks on Ukraine and Poland

Prestige Ransomware

- Targeted Poland and Supporting Countries of Poland
- Leveraged already obtained Domain Admin Creds
 - Personally suspect that targets were already compromised --- lay and wait
- 3 methods for deployment
 - Scheduled task from ADMIN\$ Share
 - Powershell Command ADMIN\$ Share
 - Distributed via Group Policy via Domain Controller

Microsoft links attack to Russian's Sandworm --- which goes back to Industroyer malware that hit the Ukranian Powergrid in 2016 ---- but later saw that they had a newer version March 2022 --- that followed initial breach in Feb 2022

coinciding with Russian invasion --- malware set to detonate April 8, 2022 but was foiled --- and then CaddyWiper was supposed to run 10 mins later to destroy forensic artifacts

<https://thehackernews.com/2022/11/over-15000-wordpress-sites-compromised.html>

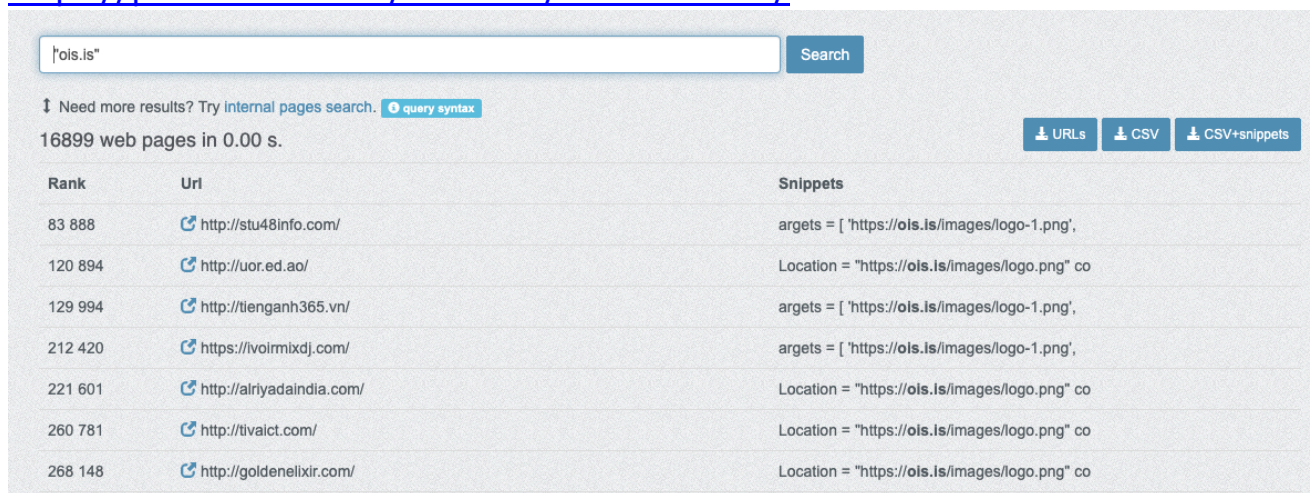
Over 15,000 WordPress Sites Compromised in Malicious SEO Campaign

Wordpress sites are compromised to redirect to Q&A site of malicious choosing --- Initial compromise was not discovered --- no signs of exploits --- suggested possible brute force or access to legit creds

Taking advantage of the Search Engine Optimization ranking to make site more legit and popular always stands as a precursor to something --- or testing/validating

- Reputation is a great catch to prevent orgs from going to bad sites
- One of the best catches I've seen is blocking sites with no category
 - o Too new
 - o Too rare
 - o Most often malicious or just bad as in terribly made unpopular sites

• <https://publicwww.com/websites/%22ois.is%22/>



↑ Need more results? Try [Internal pages search](#). [query syntax](#)

16899 web pages in 0.00 s. [URLs](#) [CSV](#) [CSV+snippets](#)

Rank	Url	Snippets
83 888	http://stu48info.com/	argets = ['https://ois.is/images/logo-1.png',
120 894	http://uor.ed.ao/	Location = "https://ois.is/images/logo.png" co
129 994	http://tienganh365.vn/	argets = ['https://ois.is/images/logo-1.png',
212 420	https://ivoirmixdj.com/	argets = ['https://ois.is/images/logo-1.png',
221 601	http://alriyadaindia.com/	Location = "https://ois.is/images/logo.png" co
260 781	http://tivaict.com/	Location = "https://ois.is/images/logo.png" co
268 148	http://goldenelixir.com/	Location = "https://ois.is/images/logo.png" co

<https://www.bleepingcomputer.com/news/security/us-health-dept-warns-of-venus-ransomware-targeting-healthcare-orgs/>

US Health Dept warns of Venus ransomware targeting

US Health Dept warns of Venus ransomware targeting healthcare orgs

Things to consider

- no associated data leak site associated with Venus --- no lines of double extortion
- Seem to really take advantage of open remote connectivity
 - o So less likely to have phishing payloads with malware
 - o More likely phishing with webpage scams for credential stealing
 - o Potential credential stuffing/brute forcing
- Things to look for in my opinion
 - o Off hour remote connections
- 2-factor is your friend is this is the common vector

"Thanks Everyone for joining our Out of the Woods Threat Hunting Podcast. Looking forward to syncing back up next week.

With that, let's dive into the Top 5 Threat Hunting Headlines for the week of Nov 14th 2022!