TTACKERS LEVERAGE EXCEL, POWERSHELL AND DNS IN LATEST NON-MALWARE ATTACK

ATTACK BACKGROUND

ATTACK TECHNICAL ANALYSIS

FIRST STAGE

```
File Name       : trill.xls
File Size       : 131,072 bytes
MD5             : 2a462cdbaee3b0340bc6298057d83240
SHA1            : 256e736d7dcb670c6a510b5a7d60a53572acc1e7
SHA256          : 0dc86ad65c90cfc84253c4d7605911aba93b599b1bbd422ce8f597f3ffd59009
```

```
Offset          0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00012490   00 00 08 40 00 1E F1 10  00 00 00 0D 00 00 08 0C     @  ñ
000124A0   00 00 08 17 00 00 08 F7  00 00 10 FC 00 20 20 27            ÷   ü   '
000124B0   00 00 00 09 00 00 00 FC  6C 00 4A 41 42 7A 41 47              ül JABzAG
000124C0   4D 41 63 67 42 70 41 48  41 41 64 41 42 6B 41 47   MAcgBpAHAAdABkAG
000124D0   6B 41 63 67 41 67 41 44  30 41 49 41 41 69 41 43   kAcgAgAD0AIAAiAC
000124E0   51 41 5A 51 42 75 41 48  59 41 4F 67 42 31 41 48   QAZQBuAHYAOgB1AH
000124F0   4D 41 5A 51 42 79 41 48  41 41 63 67 42 76 41 47   MAZQByAHAAcgBvAG
00012500   59 41 61 51 42 73 41 47  55 41 58 41 42 68 41 48   YAaQBsAGUAXABhAH
```

```
Offset          0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

000164D0   41 41 67 41 43 41 41 49  41 41 6B 41 48 4D 41 5A   AAgACAAIAAkAHMAZ
000164E0   51 42 79 41 48 59 41 5A  51 42 79 41 46 49 41 5A   QByAHYAZQByAFIAZ
000164F0   51 42 30 3C 00 20 20 00  41 41 30 41 43 67 41 4A   QB0<         AA0ACgAJ
00016500   41 41 6B 41 61 51 42 6D  41 43 41 41 4B 41 41 6B   AAkAaQBmACAAKAAk
00016510   41 48 4D 41 5A 51 42 79  41 48 59 41 5A 51 42 79   AHMAZQByAHYAZQBy
```

```
Offset          0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

000191A0   41 49 41 42 39 41 41 30  41 43 67 41 4E 41 41 6F   AIAB9AA0ACgANAAo
000191B0   41 66 51 41 4E 41 41 6F  41 5A 51 42 34 41 47 6B   AfQANAAoAZQB4AGk
000191C0   41 64 41 41 3D FC 0B 00  4A 41 42 77 41 47 45 41   AdAA=ü  JABwAGEA
000191D0   64 41 42 6F 41 44 30 41  49 41 41 69 41 43 51 41   dABoAD0AIAAiACQA
000191E0   5A 51 42 75 41 48 59 41  4F 67 42 31 41 48 4D 41   ZQBuAHYAOgB1AHMA
```

SECOND STAGE

```
File Name       : second_stage_ps1
File Size       : 1,111 bytes
MD5             : 285cd7836444d743c613c97e1448f233
SHA1            : 3e12650286702910ae0c9701a5023180a57e39dd
SHA256          : 1f2c88612c760062c441110b5ff86c844a3bd68fde217ecd43997b55824c8d0a
```

FINAL PAYLOAD

```
File Name       : mc.ps1
File Size       : 20,924 bytes
MD5             : bebb6238a9b858386cef07328f4470e3
SHA1            : ba9e9c8d36b88b6a8cbe3fa116bfb8c8e1c6c9ad
SHA256          : ec3b2e453b5c6761889d212be3b754d0761a6cedb178fd56e2e1d5d31994349d
```

```
Standard mapping        - ABCDEFGHIJKLMNOPQRSTUVWXYZ234567
```

```
Custom mapping  - abcdefghijklmnopqrstuvwxyz012345
```

```
bne_42036_8675309.yjksdrl.tk
```

```
bd_42306_1_-_txt_0_314159.yjksdrl.tk
```

5 TECHNIQUES HACKERS USE TO JAILBREAK CHATGPT, GEMINI, AND COPILOT AI SYSTEMS

THIS HACKER TOOLKIT CAN BREACH ANY AIR-GAPPED SYSTEM – HERE'S HOW IT WORKS

HACKING PAGERS TO EXPLOSIONS: ISRAEL'S COVERT CYBER-PHYSICAL SABOTAGE OPERATION AGAINST HEZBOLLAH!

FIVE TECHNIQUES FOR BYPASSING MICROSOFT SMARTSCREEN AND SMART APP CONTROL (SAC) TO RUN MALWARE IN WINDOWS

HOW MILLIONS OF PHISHING EMAILS WERE SENT FROM TRUSTED DOMAINS: ECHOSPOOFING EXPLAINED

HOW TO IMPLEMENT PRINCIPLE OF LEAST PRIVILEGE(CLOUD SECURITY) IN AWS, AZURE, AND GCP CLOUD

Alisa Esage G

Working as a cyber security solutions architect, Alisa focuses on application and network security. Before joining us she held a cyber security researcher positions within a variety of cyber security start-ups. She also experience in different industry domains like finance, healthcare and consumer products.

TUNNELCRACK: TWO SERIOUS VULNERABILITIES IN VPNS DISCOVERED, HAD BEEN DORMANT SINCE 1996

HOW TO EASILY HACK TP-LINK ARCHER AX21 WI-FI ROUTER

US GOVT WANTS NEW LABEL ON SECURE IOT DEVICES OR WANTS TO DISCOURAGE USE OF CHINESE IOT GADGETS

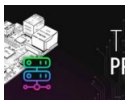
24,649,096,027 (24.65 BILLION) ACCOUNT USERNAMES AND PASSWORDS HAVE BEEN LEAKED BY CYBER CRIMINALS TILL NOW IN 2022

HOW CHINESE APT HACKERS STOLE LOCKHEED MARTIN F-35 FIGHTER PLANE TO DEVELOP ITS OWN J-20 STEALTH FIGHTER AIRCRAFT [VIDEO]

MASSIVE NVIDIA GPU EXPLOIT FOUND. HOW HACKERS CAN TAKE DOWN 35% OF AI SYSTEMS IN CLOUD!

BLAST-RADIUS ATTACK EXPLOTING CRITICAL RADIUS FLAW COULD COMPROMISE YOUR NETWORK

14 MILLION SERVERS VULNERABLE TO CRITICAL OPENSSH BUG: BECOME REMOTE ADMIN WITH CVE-2024-6387



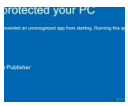
HOW SAFE IS YOUR TINYPROXY? STEP-BY-STEP GUIDE TO EXPLOITING TINYPROXY'S ZERO DAY VULNERABILITY

ETERNAL MALWARE: CVE-2024-3400 ROOTKITS PERSIST THROUGH PALO ALTO FIREWALLS UPDATES AND RESETS

5 TECHNIQUES HACKERS USE TO JAILBREAK CHATGPT, GEMINI, AND COPILOT AI SYSTEMS

THIS HACKER TOOLKIT CAN BREACH ANY AIR-GAPPED SYSTEM – HERE'S HOW IT WORKS

HACKING PAGERS TO EXPLOSIONS: ISRAEL'S COVERT CYBER-PHYSICAL SABOTAGE OPERATION AGAINST HEZBOLLAH!



FIVE TECHNIQUES FOR BYPASSING MICROSOFT SMARTSCREEN AND SMART APP CONTROL (SAC) TO RUN MALWARE IN WINDOWS

HOW MILLIONS OF PHISHING EMAILS WERE SENT FROM TRUSTED DOMAINS: ECHOSPOOFING EXPLAINED

HOW TO IMPLEMENT PRINCIPLE OF LEAST PRIVILEGE(CLOUD SECURITY) IN AWS, AZURE, AND GCP CLOUD

THE 11 ESSENTIAL FALCO CLOUD SECURITY RULES FOR SECURING CONTAINERIZED APPLICATIONS AT NO COST

HACK-PROOF YOUR CLOUD: THE STEP-BY-STEP CONTINUOUS THREAT EXPOSURE MANAGEMENT CTEM STRATEGY FOR AWS & AZURE

WEB-BASED PLC MALWARE: A NEW TECHNIQUE TO HACK INDUSTRIAL CONTROL SYSTEMS

THE API SECURITY CHECKLIST: 10 STRATEGIES TO KEEP API INTEGRATIONS SECURE

THIS HACKER TOOLKIT CAN BREACH ANY AIR-GAPPED SYSTEM – HERE'S HOW IT WORKS

HACKERS' GUIDE TO ROGUE VM DEPLOYMENT: LESSONS FROM THE MITRE HACK

ETERNAL MALWARE: CVE-2024-3400 ROOTKITS PERSIST THROUGH PALO ALTO FIREWALLS UPDATES AND RESETS

MAJOR PYTHON INFRASTRUCTURE BREACH – OVER 170K USERS COMPROMISED. HOW SAFE IS YOUR CODE?

HOW TO EXPLOIT WINDOWS DEFENDER ANTIVIRUS TO INFECT A DEVICE WITH MALWARE

US GOVT WANTS NEW LABEL ON SECURE IOT DEVICES OR WANTS TO DISCOURAGE USE OF CHINESE IOT GADGETS

24,649,096,027 (24.65 BILLION) ACCOUNT USERNAMES AND PASSWORDS HAVE BEEN LEAKED BY CYBER CRIMINALS TILL NOW IN 2022

HOW CHINESE APT HACKERS STOLE LOCKHEED MARTIN F-35 FIGHTER PLANE TO DEVELOP ITS OWN J-20 STEALTH FIGHTER AIRCRAFT [VIDEO]