Earth Lusca, TAG-22, Charcoal Typhoon, CHROMIUM, ControlX, Group G1006

Archived: 2026-04-05 15:08:51 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

Earth Lusca has used the Fodhelper UAC bypass technique to gain elevated privileges.[1]

Enterprise T1098 .004 Account Manipulation: SSH Authorized Keys

Earth Lusca has dropped an SSH-authorized key in the `/root/.ssh` folder in order to access a compromised server with SSH.[1]

Enterprise T1583 .001 Acquire Infrastructure: Domains

Earth Lusca has registered domains, intended to look like legitimate target domains, that have been used in watering hole attacks.[1]

.004 Acquire Infrastructure: Server

Earth Lusca has acquired multiple servers for some of their operations, using each server for a different role.[1]

.006 Acquire Infrastructure: Web Services

Earth Lusca has established GitHub accounts to host their malware.[1]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

Earth Lusca has scanned for vulnerabilities in the public-facing servers of their targets.[1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Earth Lusca has used WinRAR to compress stolen files into an archive prior to exfiltration.[1]

Enterprise T1547 .012 Boot or Logon Autostart Execution: Print Processors

Earth Lusca has added the Registry key `HKLM\SYSTEM\ControlSet001\Control\Print\Environments\Windows x64\Print Processors\UDPrint" /v Driver /d "spool.dll /f` to load malware as a Print Processor.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Earth Lusca has used PowerShell to execute commands.[1]

.005 Command and Scripting Interpreter: Visual Basic

Earth Lusca used VBA scripts.[1]

.006 Command and Scripting Interpreter: Python

Earth Lusca used Python scripts for port scanning or building reverse shells.[1]

.007 Command and Scripting Interpreter: JavaScript

Earth Lusca has manipulated legitimate websites to inject malicious JavaScript code as part of their watering hole operations.[1]

Enterprise T1584 .004 Compromise Infrastructure: Server

Earth Lusca has used compromised web servers as part of their operational infrastructure.[1]

.006 Compromise Infrastructure: Web Services

Earth Lusca has compromised Google Drive repositories.[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Earth Lusca created a service using the command `sc create "SysUpdate" binpath= "cmd /c start "[file path]""&&sc config "SysUpdate" start= auto&&net start SysUpdate` for persistence.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Earth Lusca has used certutil to decode a string into a cabinet file.[1]

Enterprise T1482 Domain Trust Discovery

Earth Lusca has used Nltest to obtain information about domain controllers.[1]

Enterprise T1189 Drive-by Compromise

Earth Lusca has performed watering hole attacks.[1]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

Earth Lusca has used the megacmd tool to upload stolen files from a victim network to MEGA.[1]

Enterprise T1190 Exploit Public-Facing Application

Earth Lusca has compromised victims by directly exploiting vulnerabilities of public-facing servers, including those associated with Microsoft Exchange and Oracle GlassFish.[1]

Enterprise T1210 Exploitation of Remote Services

Earth Lusca has used Mimikatz to exploit a domain controller via the ZeroLogon exploit (CVE-2020-1472).[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Earth Lusca has placed a malicious payload in `%WINDIR%\SYSTEM32\oci.dll` so it would be sideloaded by the MSDTC service.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Earth Lusca used the command `move [file path] c:\windows\system32\spool\prtprocs\x64\spool.dll` to move and register a malicious DLL name as a Windows print processor, which eventually was loaded by the Print Spooler service.[1]

Enterprise T1112 Modify Registry

Earth Lusca modified the registry using the command `reg add "HKEY_CURRENT_USER\Environment" /v UserInitMprLogonScript /t REG_SZ /d "[file path]"` for persistence.[1]

Enterprise T1027 Obfuscated Files or Information

Earth Lusca used Base64 to encode strings.[1]

.003 Steganography

Earth Lusca has used steganography to hide shellcode in a BMP image file.[1]

Enterprise T1588 .001 Obtain Capabilities: Malware

Earth Lusca has acquired and used a variety of malware, including Cobalt Strike.[1]

.002 Obtain Capabilities: Tool

Earth Lusca has acquired and used a variety of open source tools.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Earth Lusca has used ProcDump to obtain the hashes of credentials by dumping the memory of the LSASS process.[1]

.006 OS Credential Dumping: DCSync

Earth Lusca has used a `DCSync` command with Mimikatz to retrieve credentials from an exploited controller.[1]

Enterprise T1566 .002 Phishing: Spearphishing Link

Earth Lusca has sent spearphishing emails to potential targets that contained a malicious link.[1]

Enterprise T1057 Process Discovery

Earth Lusca has used Tasklist to obtain information from a compromised host.[1]

Enterprise T1090 Proxy

Earth Lusca adopted Cloudflare as a proxy for compromised servers.[1]

Enterprise T1018 Remote System Discovery

Earth Lusca used the command `powershell "Get-EventLog -LogName security -Newest 500 | where {$_.EventID -eq 4624} | format-list -property * | findstr "Address""` to find the network information of successfully logged-in accounts to discovery addresses of other machines. Earth Lusca has also used multiple scanning tools to discover other machines within the same compromised network.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Earth Lusca used the command `schtasks /Create /SC ONLOgon /TN WindowsUpdateCheck /TR "[file path]" /ru system` for persistence.[1]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

Earth Lusca has staged malware and malicious files on compromised web servers, GitHub, and Google Drive.[1]

Enterprise T1218 .005 System Binary Proxy Execution: Mshta

Earth Lusca has used `mshta.exe` to load an HTA script within a malicious .LNK file.[1]

Enterprise T1016 System Network Configuration Discovery

Earth Lusca used the command `ipconfig` to obtain information about network configurations.[1]

Enterprise T1049 System Network Connections Discovery

Earth Lusca employed a PowerShell script called RDPConnectionParser to read and filter the Windows event log "Microsoft-Windows-TerminalServices-RDPClient/Operational"
(Event ID 1024) to obtain network information from RDP connections. Earth Lusca has also used netstat from a compromised system to obtain network connection information.[1]

Enterprise T1033 System Owner/User Discovery

Earth Lusca collected information on user accounts via the `whoami` command.[1]

Enterprise T1007 System Service Discovery

Earth Lusca has used Tasklist to obtain information from a compromised host.[1]

Enterprise T1204 .001 User Execution: Malicious Link

Earth Lusca has sent spearphishing emails that required the user to click on a malicious link and subsequently open a decoy document with a malicious loader.[1]

.002 User Execution: Malicious File

Earth Lusca required users to click on a malicious file for the loader to activate.[1]

Enterprise T1047 Windows Management Instrumentation

Earth Lusca used a VBA script to execute WMI.[1]
