# Magic Hound, TA453, COBALT ILLUSION, Charming Kitten, ITG18, Phosphorus, Newscaster, APT35, Mint Sandstorm, Group G0059



Enterprise T1087 .003 Account Discovery: Email Account

Magic Hound has used Powershell to discover email accounts.[17]

Enterprise T1098 .002 Account Manipulation: Additional Email Delegate Permissions

Magic Hound granted compromised email accounts read access to the email boxes of additional targeted accounts. The group then was able to authenticate to the intended victim's OWA (Outlook Web Access) portal and read hundreds of email communications for information on Middle East organizations.[1]

.007 Account Manipulation: Additional Local or Domain Groups

Magic Hound has added a user named DefaultAccount to the Administrators and Remote Desktop Users groups.[17]

Enterprise T1583 .001 Acquire Infrastructure: Domains

Magic Hound has registered fraudulent domains such as "mail-newyorker.com" and "news12.com.recover-session-service.site" to target specific victims with phishing attacks.[3]

.006 Acquire Infrastructure: Web Services

Magic Hound has acquired Amazon S3 buckets to use in C2.[7]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

Magic Hound has conducted widespread scanning to identify public-facing systems vulnerable to CVE-2021-44228 in Log4j and ProxyShell vulnerabilities; CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 in on-premises MS Exchange Servers; and CVE-2018-13379 in Fortinet FortiOS SSL VPNs.[7][18]

Enterprise T1071 Application Layer Protocol

Magic Hound malware has used IRC for C2.[15][19]

.001 Web Protocols

Magic Hound has used HTTP for C2.[15][17][19]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Magic Hound has used gzip to archive dumped LSASS process memory and RAR to stage and compress local folders.[1][17][19]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Magic Hound malware has used Registry Run keys to establish persistence.[15][19][18]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Magic Hound has used PowerShell for execution and privilege escalation.[15][1][17][19][18]

.003 Command and Scripting Interpreter: Windows Command Shell

Magic Hound has used the command-line interface for code execution.[15][17][19]

.005 Command and Scripting Interpreter: Visual Basic

Magic Hound malware has used VBS scripts for execution.[15]

Enterprise T1586 .002 Compromise Accounts: Email Accounts

Magic Hound has compromised personal email accounts through the use of legitimate credentials and gathered additional victim information.[11]

Enterprise T1584 .001 Compromise Infrastructure: Domains

Magic Hound has used compromised domains to host links targeted to specific phishing victims.[2][5][3][20]

Enterprise T1136 .001 Create Account: Local Account

Magic Hound has created local accounts named `help` and `DefaultAccount` on compromised machines.[17][18]

Enterprise T1486 Data Encrypted for Impact

Magic Hound has used BitLocker and DiskCryptor to encrypt targeted workstations. [19][18]

Enterprise T1005 Data from Local System

Magic Hound has used a web shell to exfiltrate a ZIP file containing a dump of LSASS memory on a compromised machine.[17][19]

Enterprise T1482 Domain Trust Discovery

Magic Hound has used a web shell to execute `nltest /trusted_domains` to identify trust relationships.[19]

Enterprise T1189 Drive-by Compromise

Magic Hound has conducted watering-hole attacks through media and magazine websites.[2]

Enterprise T1114 Email Collection

Magic Hound has compromised email credentials in order to steal sensitive data.[3]

.001 Local Email Collection

Magic Hound has collected .PST archives.[1]

.002 Remote Email Collection

Magic Hound has exported emails from compromised Exchange servers including through use of the cmdlet `New-MailboxExportRequest.` [17][19]

Enterprise T1573 Encrypted Channel

Magic Hound has used an encrypted http proxy in C2 communications.[19]

Enterprise T1585 .001 Establish Accounts: Social Media Accounts

Magic Hound has created fake LinkedIn and other social media accounts to contact targets and convince them--through messages and voice communications--to open malicious links.[2]

.002 Establish Accounts: Email Accounts

Magic Hound has established email accounts using fake personas for spearphishing operations.[11][6]

Enterprise T1567 Exfiltration Over Web Service

Magic Hound has used the Telegram API `sendMessage` to relay data on compromised devices.[20]

Enterprise T1190 Exploit Public-Facing Application

Magic Hound has exploited the Log4j utility (CVE-2021-44228), on-premises MS Exchange servers via "ProxyShell" (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), and Fortios SSL VPNs (CVE-2018-13379).[7][17][21][19][18][22]

Enterprise T1083 File and Directory Discovery

Magic Hound malware can list a victim's logical drives and the type, as well the total/free space of the fixed devices. Other malware can list a directory's contents.[15]

Enterprise T1592 .002 Gather Victim Host Information: Software

Magic Hound has captured the user-agent strings from visitors to their phishing sites.[20]

Enterprise T1589 Gather Victim Identity Information

Magic Hound has acquired mobile phone numbers of potential targets, possibly for mobile malware or additional phishing operations.[5]

.001 Credentials

Magic Hound gathered credentials from two victims that they then attempted to validate across 75 different websites. Magic Hound has also collected credentials from over 900 Fortinet VPN servers in the US, Europe, and Israel.[11][18]

.002 Email Addresses

Magic Hound has identified high-value email accounts in academia, journalism, NGO's, foreign policy, and national security for targeting.[5][20]

Enterprise T1590 .005 Gather Victim Network Information: IP Addresses

Magic Hound has captured the IP addresses of visitors to their phishing sites.[20]

Enterprise T1591 .001 Gather Victim Org Information: Determine Physical Locations

Magic Hound has collected location information from visitors to their phishing sites.[20]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Magic Hound malware has a function to determine whether the C2 server wishes to execute the newly dropped file in a hidden window.[15]

Enterprise T1562 Impair Defenses

Magic Hound has disabled LSA protection on compromised hosts using `"reg" add HKLM\SYSTEM\CurrentControlSet\Control\LSA /v RunAsPPL /t REG_DWORD /d 0 /f`.[17]

.001 Disable or Modify Tools

Magic Hound has disabled antivirus services on targeted systems in order to upload malicious payloads.[17]

.002 Disable Windows Event Logging

Magic Hound has executed scripts to disable the event log service.[19]

.004 Disable or Modify System Firewall

Magic Hound has added the following rule to a victim's Windows firewall to allow RDP traffic - `"netsh" advfirewall firewall add rule name="Terminal Server" dir=in action=allow protocol=TCP localport=3389`. [17][19]

Enterprise T1070 .003 Indicator Removal: Clear Command History

Magic Hound has removed mailbox export requests from compromised Exchange servers.[17]

.004 Indicator Removal: File Deletion

Magic Hound has deleted and overwrote files to cover tracks.[15][1][19]

Enterprise T1105 Ingress Tool Transfer

Magic Hound has downloaded additional code and files from servers onto victims.[15][17][19][18]

Enterprise T1056 .001 Input Capture: Keylogging

Magic Hound malware is capable of keylogging.[15]

Enterprise T1570 Lateral Tool Transfer

Magic Hound has copied tools within a compromised network using RDP.[19]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Magic Hound has named a malicious script CacheTask.bat to mimic a legitimate task.[19]

.005 Masquerading: Match Legitimate Resource Name or Location

Magic Hound has used `dllhost.exe` to mask Fast Reverse Proxy (FRP) and `MicrosoftOutLookUpdater.exe` for Plink.[17][19][18]

.010 Masquerading: Masquerade Account Name

Magic Hound has created local accounts named `help` and `DefaultAccount` on compromised machines.[17][18]

Enterprise T1112 Modify Registry

Magic Hound has modified Registry settings for security tools.[17]

Enterprise T1046 Network Service Discovery

Magic Hound has used KPortScan 3.0 to perform SMB, RDP, and LDAP scanning.[19]

Enterprise T1571 Non-Standard Port

Magic Hound malware has communicated with its C2 server over TCP ports 4443 and 10151 using HTTP.[15][19]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Magic Hound has used base64-encoded commands.[15][18]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Magic Hound malware has used base64-encoded files and has also encrypted embedded strings with AES.[15][18]

Enterprise T1588 .002 Obtain Capabilities: Tool

Magic Hound has obtained and used tools like Havij, sqlmap, Metasploit, Mimikatz, and Plink.[23][1][7][19][18]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Magic Hound has stolen domain credentials by dumping LSASS process memory using Task Manager, comsvcs.dll, and from a Microsoft Active Directory Domain Controller using Mimikatz.[1][17][19][18]

Enterprise T1566 .002 Phishing: Spearphishing Link

Magic Hound has sent malicious URL links through email to victims. In some cases the URLs were shortened or linked to Word documents with malicious macros that executed PowerShells scripts to download Pupy.[24][2][3] [18]

.003 Phishing: Spearphishing via Service

Magic Hound used various social media channels (such as LinkedIn) as well as messaging services (such as WhatsApp) to spearphish victims.[25][12][2]

Enterprise T1598 .003 Phishing for Information: Spearphishing Link

Magic Hound has used SMS and email messages with links designed to steal credentials or track victims.[3][2][6] [5][20][18]

Enterprise T1057 Process Discovery

Magic Hound malware can list running processes.[15]

Enterprise T1572 Protocol Tunneling

Magic Hound has used Plink to tunnel RDP over SSH.[19]

Enterprise T1090 Proxy

Magic Hound has used Fast Reverse Proxy (FRP) for RDP traffic.[19]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Magic Hound has used Remote Desktop Services to copy tools on targeted systems.[17][19]

Enterprise T1018 Remote System Discovery

Magic Hound has used Ping for discovery on targeted networks.[19]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Magic Hound has used scheduled tasks to establish persistence and execution.[17][19]

Enterprise T1113 Screen Capture

Magic Hound malware can take a screenshot and upload the file to its C2 server.[15]

Enterprise T1505 .003 Server Software Component: Web Shell

Magic Hound has used multiple web shells to gain execution.[17][19]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Magic Hound has used rundll32.exe to execute MiniDump from comsvcs.dll when dumping LSASS memory.[17]

Enterprise T1082 System Information Discovery

Magic Hound malware has used a PowerShell command to check the victim system architecture to determine if it is an x64 machine. Other malware has obtained the OS version, UUID, and computer/host name to send to the C2 server.[15][17][19]

Enterprise T1016 System Network Configuration Discovery

Magic Hound malware gathers the victim's local IP address, MAC address, and external IP address.[15][17][19]

.001 Internet Connection Discovery

Magic Hound has conducted a network call out to a specific website as part of their initial discovery activity.[19]

.002 Wi-Fi Discovery

Magic Hound has collected names and passwords of all Wi-Fi networks to which a device has previously connected.[7]

Enterprise T1049 System Network Connections Discovery

Magic Hound has used quser.exe to identify existing RDP connections.[17]

Enterprise T1033 System Owner/User Discovery

Magic Hound malware has obtained the victim username and sent it to the C2 server.[15][17][19]

Enterprise T1204 .001 User Execution: Malicious Link

Magic Hound has attempted to lure victims into opening malicious links embedded in emails.[2][3]

.002 User Execution: Malicious File

Magic Hound has attempted to lure victims into opening malicious email attachments.[2]

Enterprise T1078 .001 Valid Accounts: Default Accounts

Magic Hound enabled and used the default system managed account, DefaultAccount, via `"powershell.exe" /c net user DefaultAccount /active:yes` to connect to a targeted Exchange server over RDP.[19]

.002 Valid Accounts: Domain Accounts

Magic Hound has used domain administrator accounts after dumping LSASS process memory.[19]

Enterprise T1102 .002 Web Service: Bidirectional Communication

Magic Hound malware can use a SOAP Web service to communicate with its C2 server.[15]

Enterprise T1047 Windows Management Instrumentation

Magic Hound has used a tool to run `cmd /c wmic computersystem get domain` for discovery.[17]

---