

Gamaredon Group, IRON TILDEN, Primitive Bear, ACTINIUM, Armageddon, Shuckworm, DEV-0157, Aqua Blizzard, Group G0047

Archived: 2026-04-05 15:57:08 UTC

Enterprise [T1583](#) [.001 Acquire Infrastructure: Domains](#)

[Gamaredon Group](#) has registered multiple domains to facilitate payload staging and C2. [\[5\]](#)[\[8\]](#)[\[10\]](#)[\[11\]](#)

[.003 Acquire Infrastructure: Virtual Private Server](#)

[Gamaredon Group](#) has used VPS hosting providers for infrastructure outside of Russia. [\[12\]](#)[\[10\]](#)[\[13\]](#)

[.006 Acquire Infrastructure: Web Services](#)

[Gamaredon Group](#) has used Cloudflare's TryCloudflare service to obtain C2 nodes. [\[11\]](#)

Enterprise [T1071](#) [.001 Application Layer Protocol: Web Protocols](#)

[Gamaredon Group](#) has used HTTP and HTTPS for C2 communications. [\[1\]](#)[\[2\]](#)[\[3\]](#)[\[4\]](#)[\[14\]](#)[\[8\]](#)[\[12\]](#)[\[10\]](#)[\[15\]](#)

Enterprise [T1119 Automated Collection](#)

[Gamaredon Group](#) has deployed scripts on compromised systems that automatically scan for interesting documents. [\[3\]](#)

Enterprise [T1020 Automated Exfiltration](#)

[Gamaredon Group](#) has used modules that automatically upload gathered documents to the C2 server. [\[3\]](#)

Enterprise [T1547](#) [.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder](#)

[Gamaredon Group](#) tools have registered Run keys in the registry to give malicious VBS files persistence. [\[2\]](#)[\[3\]](#)[\[14\]](#)
[\[12\]](#)[\[10\]](#)

Enterprise [T1059](#) [.001 Command and Scripting Interpreter: PowerShell](#)

[Gamaredon Group](#) has used obfuscated PowerShell scripts for staging. [\[5\]](#)[\[10\]](#) Additionally, (LinkById : G0047) has used PowerShell based tools later in its attack chain. [\[11\]](#) Additionally, [Gamaredon Group](#) has used the PowerShell cmdlet `Get-Command` to download and execute the next stage payload. [\[15\]](#)

[.003 Command and Scripting Interpreter: Windows Command Shell](#)

[Gamaredon Group](#) has used various batch scripts to establish C2 and download additional files. [Gamaredon Group](#)'s backdoor malware has also been written to a batch file. ^{[1][3][14][8]}

[.005 Command and Scripting Interpreter: Visual Basic](#)

[Gamaredon Group](#) has embedded malicious macros in document templates, which executed VBScript. [Gamaredon Group](#) has also delivered Microsoft Outlook VBA projects with embedded macros. ^{[2][3][14][5][7][10]} Additionally, [Gamaredon Group](#) has executed VBScript files using wscript.exe. ^[11]

Enterprise [T1005 Data from Local System](#)

[Gamaredon Group](#) has collected files from infected systems and uploaded them to a C2 server. ^{[3][10]}

Enterprise [T1039 Data from Network Shared Drive](#)

[Gamaredon Group](#) malware has collected Microsoft Office documents from mapped network drives. ^{[3][10]}

Enterprise [T1025 Data from Removable Media](#)

A [Gamaredon Group](#) file stealer has the capability to steal data from newly connected logical volumes on a system, including USB drives. ^{[1][3][10]}

Enterprise [T1001 Data Obfuscation](#)

[Gamaredon Group](#) has used obfuscated VBScripts with randomly generated variable names and concatenated strings. ^[12]

Enterprise [T1491 .001 Defacement: Internal Defacement](#)

[Gamaredon Group](#) has left taunting images and messages on the victims' desktops as proof of system access. ^[14]

Enterprise [T1140 Deobfuscate/Decode Files or Information](#)

[Gamaredon Group](#) tools decrypted additional payloads from the C2. [Gamaredon Group](#) has also decoded Base64-encoded source code of a downloader. ^{[2][3][10]} Additionally, [Gamaredon Group](#) has decoded Telegram content to reveal the IP address for C2 communications. ^[12]

Enterprise [T1587 .003 Develop Capabilities: Digital Certificates](#)

[Gamaredon Group](#) has used the same TLS certificate across its infrastructure. ^[13]

Enterprise [T1561 .001 Disk Wipe: Disk Content Wipe](#)

[Gamaredon Group](#) has used tools to delete files and folders from victims' desktops and profiles. ^[14]

Enterprise [T1568 Dynamic Resolution](#)

[Gamaredon Group](#) has incorporated dynamic DNS domains in its infrastructure. ^[8]

[.001 Fast Flux DNS](#)

[Gamaredon Group](#) has used fast flux DNS to mask their command and control channel behind rotating IP addresses.^{[12][10][16]} Additionally, [Gamaredon Group](#) has used a low-frequency variant of the single-flux method.^[13]

Enterprise [T1480 Execution Guardrails](#)

[Gamaredon Group](#) has used geoblocking to limit downloads of the malicious file to specific geographic locations.^{[12][15]}

Enterprise [T1041 Exfiltration Over C2 Channel](#)

A [Gamaredon Group](#) file stealer can transfer collected files to a hardcoded C2 server.^{[1][10][11]}

Enterprise [T1083 File and Directory Discovery](#)

[Gamaredon Group](#) macros can scan for Microsoft Word and Excel files to inject with additional malicious macros. [Gamaredon Group](#) has also used its backdoors to automatically list interesting files (such as Office documents) found on a system.^{[3][8][10]} [Gamaredon Group](#) has also identified directory trees, folders and files on the compromised host.^[11]

Enterprise [T1564 .003 Hide Artifacts: Hidden Window](#)

[Gamaredon Group](#) has used `hidcon` to run batch files in a hidden console window.^[8] [Gamaredon Group](#) has also executed PowerShell in a hidden window.^[15]

Enterprise [T1562 .001 Impair Defenses: Disable or Modify Tools](#)

[Gamaredon Group](#) has delivered macros which can tamper with Microsoft Office security settings.^{[3][10]}

Enterprise [T1070 .004 Indicator Removal: File Deletion](#)

[Gamaredon Group](#) tools can delete files used during an operation.^{[2][4][14][10]}

Enterprise [T1105 Ingress Tool Transfer](#)

[Gamaredon Group](#) has downloaded additional malware and tools onto a compromised host.^{[1][2][3][5][10][15]} For example, [Gamaredon Group](#) uses a backdoor script to retrieve and decode additional payloads once in victim environments.^[12]

Enterprise [T1559 .001 Inter-Process Communication: Component Object Model](#)

[Gamaredon Group](#) malware can insert malicious macros into documents using a `Microsoft.Office.Interop` object.^{[3][10]}

Enterprise [T1534 Internal Spearphishing](#)

[Gamaredon Group](#) has used an Outlook VBA module on infected systems to send phishing emails with malicious attachments to other employees within the organization. ^[3]

Enterprise [T1036 .005 Masquerading: Match Legitimate Resource Name or Location](#)

[Gamaredon Group](#) has used legitimate process names to hide malware including `svchosst`. ^[8] Additionally, [Gamaredon Group](#) disguised malicious ZIP archives as Office documents that are related to the invasion. ^[15]

Enterprise [T1112 Modify Registry](#)

[Gamaredon Group](#) has removed security settings for VBA macro execution by changing registry values `HKCU\Software\Microsoft\Office\<version>\<product>\Security\VBWarnings` and `HKCU\Software\Microsoft\Office\<version>\<product>\Security\AccessVBOM`. ^{[3][14][10]} [Gamaredon Group](#) has also modified Registry keys to hide folders and system files and to add the C2 address under `HKEY_CURRENT_USER\Console\WindowsUpdate`. ^[11]

Enterprise [T1106 Native API](#)

[Gamaredon Group](#) malware has used `CreateProcess` to launch additional malicious components. ^{[3][10]}

Enterprise [T1095 Non-Application Layer Protocol](#)

[Gamaredon Group](#) has used SOCKS5 over port 9050 for C2 communication. ^[11]

Enterprise [T1571 Non-Standard Port](#)

[Gamaredon Group](#) has used port 6856 for C2 communications. ^[15]

Enterprise [T1027 Obfuscated Files or Information](#)

[Gamaredon Group](#) has delivered self-extracting 7z archive files within malicious document attachments. ^[3]

Additionally, [Gamaredon Group](#) has used an obfuscated .drv file. ^[11]

[.004 Compile After Delivery](#)

[Gamaredon Group](#) has compiled the source code for a downloader directly on the infected system using the built-in `Microsoft.CSharp.CSharpCodeProvider` class. ^[3]

[.010 Command Obfuscation](#)

[Gamaredon Group](#) has used obfuscated or encrypted scripts. ^{[3][5][11][10]}

[.012 LNK Icon Smuggling](#)

[Gamaredon Group](#) has used LNK files to hide malicious scripts for execution. ^{[11][15]}

[.015 Compression](#)

[Gamaredon Group](#) has delivered malicious payloads within compressed archives and zip files. ^[15]

[.016 Junk Code Insertion](#)

[Gamaredon Group](#) has obfuscated .NET executables by inserting junk code. ^[3]

Enterprise [T1588 .002 Obtain Capabilities: Tool](#)

[Gamaredon Group](#) has used various legitimate tools, such as `mshta.exe` and [Reg](#), and services during operations. ^{[12][10]}

Enterprise [T1137 Office Application Startup](#)

[Gamaredon Group](#) has inserted malicious macros into existing documents, providing persistence when they are reopened. [Gamaredon Group](#) has loaded the group's previously delivered VBA project by relaunching Microsoft Outlook with the `/altvba` option, once the Application.Startup event is received. ^[3]

Enterprise [T1120 Peripheral Device Discovery](#)

[Gamaredon Group](#) tools have contained an application to check performance of USB flash drives. [Gamaredon Group](#) has also used malware to scan for removable drives. ^{[1][3][10]}

Enterprise [T1566 .001 Phishing: Spearphishing Attachment](#)

[Gamaredon Group](#) has delivered spearphishing emails with malicious attachments to targets. ^{[2][3][14][5][8][7][12][10][16]} Additionally, [Gamaredon Group](#) has distributed malicious LNK files compressed in ZIP archives. ^[15]

Enterprise [T1057 Process Discovery](#)

[Gamaredon Group](#) has used tools to enumerate processes on target hosts including Process Explorer. ^{[4][8][11]}

Enterprise [T1055 Process Injection](#)

[Gamaredon Group](#) has injected [Remcos](#) into explorer.exe. ^[15]

Enterprise [T1090 Proxy](#)

[Gamaredon Group](#) has used the Cloudflare Tunnel client to proxy C2 traffic. ^[10]

[.003 Multi-hop Proxy](#)

[Gamaredon Group](#) has used [Tor](#) for C2 traffic. ^[11]

Enterprise [T1012 Query Registry](#)

[Gamaredon Group](#) has queried `HKEY_CURRENT_USER\Console\WindowsUpdates` to obtain the C2 addresses. ^[11]

[Gamaredon Group](#) has queried `HKEY_CURRENT_USER\Console\WindowsUpdates` to obtain the C2 addresses. ^[11]

Enterprise [T1620 Reflective Code Loading](#)

[Gamaredon Group](#) has used an obfuscated PowerShell script that used `System.Reflection.Assembly` to gather and send victim information to the C2.^[11]

Enterprise [T1021 .005 Remote Services: VNC](#)

[Gamaredon Group](#) has used VNC tools, including UltraVNC, to remotely interact with compromised hosts.^{[4][5][8]}

Enterprise [T1091 Replication Through Removable Media](#)

[Gamaredon Group](#) has replicated to removable media by leveraging the User Assist Reg Key and creating LNKs on all network and removable drives available on the infected host.^[11]

Enterprise [T1053 .005 Scheduled Task/Job: Scheduled Task](#)

[Gamaredon Group](#) has created scheduled tasks to launch executables after a designated number of minutes have passed.^{[3][14][5][12]}

Enterprise [T1113 Screen Capture](#)

[Gamaredon Group](#)'s malware can take screenshots of the compromised computer every minute.^{[3][11][10]}

Enterprise [T1518 .001 Software Discovery: Security Software Discovery](#)

[Gamaredon Group](#) has used PowerShell scripts to identify security software on the victim machine.^[11]

Enterprise [T1608 .001 Stage Capabilities: Upload Malware](#)

[Gamaredon Group](#) has registered domains to stage payloads.^{[5][8]}

Enterprise [T1218 .005 System Binary Proxy Execution: Mshta](#)

[Gamaredon Group](#) has used `mshta.exe` to execute malicious files.^{[4][12][10][11]}

[.011 System Binary Proxy Execution: Rundll32](#)

[Gamaredon Group](#) malware has used rundll32 to launch additional malicious components.^[3]

Enterprise [T1082 System Information Discovery](#)

A [Gamaredon Group](#) file stealer can gather the victim's computer name and drive serial numbers to send to a C2 server.^{[1][2][14][11][10]}

Enterprise [T1016 .001 System Network Configuration Discovery: Internet Connection Discovery](#)

[Gamaredon Group](#) has tested connectivity between a compromised machine and a C2 server using [Ping](#) with commands such as `CSIDL_SYSTEM\cmd.exe /c ping -n 1`.^[4] [Gamaredon Group](#) has searched the ping records to obtain the C2 address and has used ping to search for the C2's status.^[11]

Enterprise [T1033 System Owner/User Discovery](#)

A [Gamaredon Group](#) file stealer can gather the victim's username to send to a C2 server.^[1]

Enterprise [T1080 Taint Shared Content](#)

[Gamaredon Group](#) has injected malicious macros into all Word and Excel documents on mapped network drives.^[3]

Enterprise [T1221 Template Injection](#)

[Gamaredon Group](#) has used DOCX files to download malicious DOT document templates and has used RTF template injection to download malicious payloads.^[17] [Gamaredon Group](#) can also inject malicious macros or remote templates into documents already present on compromised systems.^{[2][3][14][5][8][7][10]}

Enterprise [T1204 .001 User Execution: Malicious Link](#)

[Gamaredon Group](#) has attempted to get users to click on a link pointing to a malicious HTML file leading to follow-on malicious content.^{[12][10]}

[.002 User Execution: Malicious File](#)

[Gamaredon Group](#) has attempted to get users to click on Office attachments with malicious macros embedded.^{[2][3][4][14][5][8][7][12]} [Gamaredon Group](#) has also attempted to get users to click on thematically named files.^[15]

Enterprise [T1497 .001 Virtualization/Sandbox Evasion: System Checks](#)

[Gamaredon Group](#) has checked existing conditions, such as geographic location, device type, or system specification, before the victim is sent a malicious Word document.^[16]

Enterprise [T1102 Web Service](#)

[Gamaredon Group](#) has used GitHub repositories for downloaders which will be obtained by the group's .NET executable on the compromised system.^[3]

[.002 Bidirectional Communication](#)

[Gamaredon Group](#) has used several ways to try to resolve the C2 server, including: public third-party websites, an adversary-operated Telegraph channel, the [ngrok](#) utility and the TXT record of a hardcoded C2 domain.^{[10][11]}

[.003 One-Way Communication](#)

[Gamaredon Group](#) has used Telegram Messenger content to discover the IP address for C2 communications.^[12]

Enterprise [T1047 Windows Management Instrumentation](#)

[Gamaredon Group](#) has used WMI to execute scripts used for discovery and for determining the C2 IP address.^{[14][12][11][10]} [Gamaredon Group](#) has used the following WMI query to search for a ping record: `Select * From Win32_PingStatus where Address = 'mil.gov.ua'`.^[11]

Source: <https://attack.mitre.org/groups/G0047>