Threat actor leverages coin miner techniques to stay under the radar – here's how to spot them

microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them

November 30, 2020

Cryptocurrency miners are typically associated with cybercriminal operations, not sophisticated nation state actor activity. They are not the most sophisticated type of threats, which also means that they are not among the most critical security issues that defenders address with urgency. Recent campaigns from the nation-state actor BISMUTH take advantage of the low-priority alerts coin miners cause to try and fly under the radar and establish persistence.

BISMUTH, which shares similarities with OceanLotus or APT32, has been running increasingly complex cyberespionage attacks as early as 2012, using both custom and open-source tooling to target large multinational corporations, governments, financial services, educational institutions, and human and civil rights organizations. But in campaigns from July to August 2020, the group deployed Monero coin miners in attacks that targeted both the private sector and government institutions in France and Vietnam.

Because BISMUTH's attacks involved techniques that ranged from typical to more advanced, devices with common threat activities like phishing and coin mining should be elevated and inspected for advanced threats. More importantly, organizations should prioritize reducing attack surface and hardening networks against the full range of attacks. In this blog, we'll provide in-depth technical details about the BISMUTH attacks in July and August 2020 and mitigation recommendations for building organizational resilience.

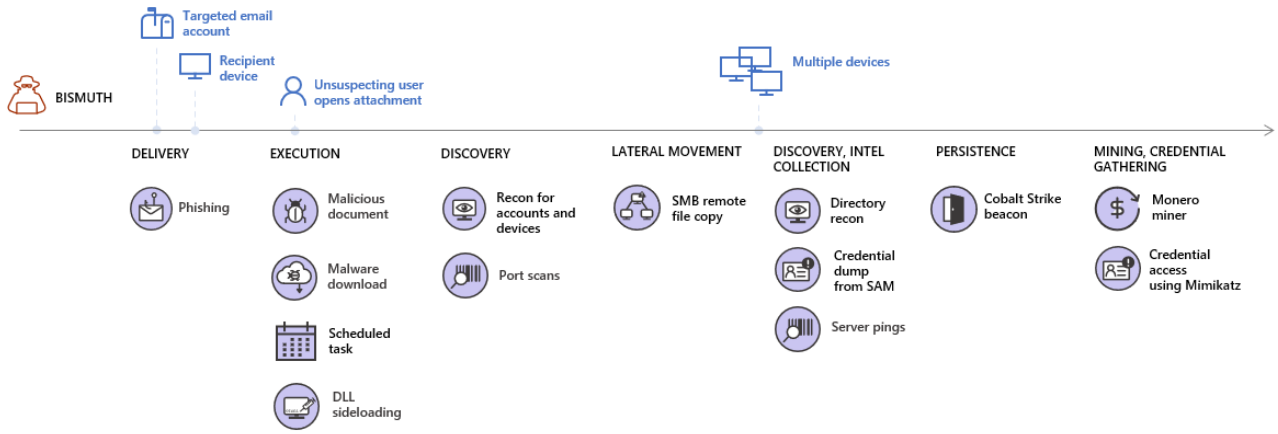
While this actor's operational goals remained the same—establish continuous monitoring and espionage, exfiltrating useful information as is it surfaced—their deployment of coin miners in their recent campaigns provided another way for the attackers to monetize compromised networks. Considering some of the group's traditional targets are human and civil rights organizations, BISMUTH attacks demonstrate how attackers give little regard to services they impact.

The use of coin miners by BISMUTH was unexpected, but it was consistent with the group's longtime methods of blending in. This pattern of blending in is particularly evident in these recent attacks, starting from the initial access stage: spear-phishing emails that were specially crafted for one specific recipient per target organization and showed signs of prior reconnaissance. In some instances, the group even corresponded with the targets, building even more believability to convince targets to open the malicious attachment and start the infection chain.

The other way that BISMUTH attempted to blend in and hide in plain sight was the heavy use of DLL side-loading, a technique in which a legitimate DLL is replaced with a malicious one so that the latter is loaded when the associated application is run. In their recent attacks, BISMUTH utilized copies of various legitimate software to load malicious DLL files and perform tasks in the context of these legitimate applications. To perform DLL sideloading, BISMUTH introduced outdated versions of various applications, including Microsoft Defender Antivirus. They also leveraged the Sysinternals DebugView tool, the McAfee on-demand scanner, and Microsoft Word 2007.

Blending in was important for BISMUTH because the group spent long periods of time performing discovery on compromised networks until they could access and move laterally to high-value targets like servers, where they installed various tools to further propagate or perform more actions. At this point in the attack, the group relied heavily on evasive PowerShell scripts, making their activities even more covert.

The coin miners also allowed BISMUTH to hide its more nefarious activities behind threats that may be perceived to be less alarming because they're "commodity" malware. If we learned anything from "commodity" banking trojans that bring in human-operated ransomware, we know that common malware infections can be indicators of more sophisticated cyberattacks and should be treated with urgency and investigated and resolved comprehensively.



Initial access

BISMUTH attempted to gain initial access by sending specially crafted malicious emails from a Gmail account that appears to have been made specifically for this campaign. It's likely the group conducted reconnaissance using publicly available sources and chose individual

targets based on their job function. Each email was sent to only one recipient at each target organization and used tailored subject lines and lure themes, for example:

- Dự thảo hợp đồng (translates from Vietnamese to "Draft Contract")
- Ứng tuyển – Trưởng ban nghiên cứu thị trường (translates from Vietnamese to "Application form – Head of Market Research")

Of note, the group sent several replies to one of these emails, which indicated that they corresponded with some targets before convincing them to open the malicious document attachment and inadvertently launch the payload. When opened, the malicious *.doc* file dropped several files in the hidden *ProgramData* folder: (1) *MpSvc.dll*, a malicious DLL with the same name as a legitimate Microsoft Defender Antivirus DLL, and (2) a copy of *MsMpEng.exe* the legitimate Microsoft Defender Antivirus executable.

The malicious document then added a scheduled task that launched the *MsMpEng.exe*copy and sideloaded the malicious *MpSvc.dll*. Because the latest versions of Microsoft Defender Antivirus are no longer susceptible to DLL sideloading, BISMUTH used an older copy to load the malicious DLL and establish a persistent command-and-control (C2) channel to the compromised device and consequently the network.

Using the newly established channel, the group dropped several files for the next stages of the attack, including a *.7z* archive, a copy of Word 2007, and another DLL, *wwlib.dll*. While it used the same name as a legitimate Microsoft Word DLL, *wwlib.dll* was a copy of KerrDown, a family of custom malware exclusive to BISMUTH. This file was subsequently sideloaded by the dropped copy of Word 2007—a technique used by BISMUTH extensively to load malicious code from a DLL file in the context of a legitimate process like *winword.exe*.

BISMUTH established another persistence method by dropping another copy of Word 2007 in a subfolder in *ProgramData*. The group then created a scheduled task that launched that copy in the same malicious manner every 60 minutes – further increasing their chances of going undetected and maintaining their presence.

Discovery

Once established as a scheduled task, the co-opted Word 2007 process dropped and loaded a scanning tool popular among attackers, *NbtScan.exe*. BISMUTH then immediately used the scanning tool to scan an IP address range within the organization. Following this network scan, the Word 2007 process launched a malicious script using a living-off-the-land-binary, *rundll32.exe*, resulting in a scan on a myriad of common ports, including 21, 22, 389, 139, and 1433. BISMUTH listed devices with open ports in a *.csv* file.

While network scanning was underway, the group performed other reconnaissance activities. They gathered information about domain and local administrators, checked whether users had local administrative privileges, and collected device information—aggregating results in a *.csv* for exfiltration. In addition, the group once again used *MsMpEng.exe* with the malicious sideloaded DLL to connect to another device that appears to have been designated by BISMUTH at some point during the attack as an internal C2 foothold and exfiltration staging device.

Continued lateral movement, discovery, and intel gathering

After a month of continual discovery on compromised devices, the group moved laterally to a server and copied over a malicious DLL that masqueraded as the system file *mpr.dll* and a copy of the Sysinternals DebugView tool. They dropped the tool onto different devices using SMB remote file copy, using file names related to popular Japanese video game characters and a seemingly random word. The actors then registered and launched malicious services multiple times, launching DebugView tool to connect to multiple Yahoo websites and confirm Internet connectivity, followed by a connection to their C2 infrastructure.

At this point, BISMUTH switched to running their attacks using PowerShell, quickly launching multiple script cmdlets. First, they dumped credentials from the Security Account Manager (SAM) database using the Empire PowerDump command and then quickly deleted PowerShell event logs to erase records generated by Script Block Logging. They then continued their discovery efforts using a PowerShell script that gathered user and group information and sent the gathered data to *.csv* files.

The script collected the following information about each user:

description, distinguishedname, lastlogontimestamp, logoncount, mail, name, primarygroupid, pwdlastset, samaccountname, userprincipalname, whenchanged, whencreated

And the following information about each domain group:

adspath, description, distinguishedname, groupType, instancetype, mail, member, memberof, name, objectsid, samaccountname,whenchanged, whencreated

Next, the group exported directory forest and domain organizational unit (OU) information. They then started connecting to dozens of devices using WMI. Following that, they collected credentials by dumping security logs under Event ID 680, possibly targeting logs related to NTLM fallbacks. Lastly, the group used the system tool *Nltest.exe* to gather domain trust info and pinged multiple servers they have identified by name during reconnaissance. Some of these servers appear to be database and file servers that could have contained high-value information for espionage objectives typically pursued by BISMUTH.

BISMUTH then installed a Cobalt Strike beacon. The group dropped a *.rar* file and extracted its contents—*McOds.exe*, which is a copy of the McAfee on-demand scanner, and a malicious DLL—into the *SysWOW64* folder. The group then created a scheduled task that launched the copy of the McAfee on-demand scanner with SYSTEM privileges and sideloaded the malicious DLL. This persistence mechanism established a connection to their Cobalt Strike server infrastructure. To clean up evidence, they deleted the dropped McAfee binary.

In terms of targets for this campaign, there were some commonalities among targets located in Vietnam that Microsoft has assessed to be tied to their previous designation as state-owned enterprises (SOEs). The observed BISMUTH activity in Vietnam targeted organizations that included former SOEs previously operated by the government of Vietnam, entities that have acquired a significant portion of a former SOE, and entities that conduct transactions with a Vietnamese government agency. Although the group's specific objectives for these recent attacks cannot be defined with high confidence, BISMUTH's past activities have included operations in support of broader espionage goals.

Coin miner deployment and credential theft

As mentioned, BISMUTH deployed coin miners during these attacks. To do this, they first dropped a *.dat* file and loaded the file using *rundll32.exe*, which in turn downloaded a copy of the 7-zip tool named *7za.exe* and a ZIP file. They then used 7-Zip to extract a Monero coin miner from the ZIP file and registered the miner as a service named after a common Virtual Machine process. Each coin miner they deployed had a unique wallet address that earned over a thousand U.S. dollars combined during the attacks.

After deploying coin miners as their distraction technique, BISMUTH then focused much of its efforts on credential theft. They registered multiple malicious services that used *%comspec%*—a relative reference to *cmd.exe* commonly used by attackers—to run the renamed DebugView tool while loading a malicious DLL. The group used DebugView and the malicious DLL in a fairly unexpected fashion to launch Base64-encoded Mimikatz commands using one of several Windows processes: *makecab.exe*, *systray.exe*, *w32tm.exe*, *bootcfg.exe*, *diskperf.exe*, *esentutl.exe*, and *typeperf.exe*.

They ran the following Mimikatz commands that require SYSTEM or Debug privileges:

- *sekurlsa::logonpasswords full*–lists all account and user password hashes, typically user and computer credentials for recently logged on users
- *lsadump::lsa /inject*—injects LSASS to retrieve credentials and request the LSA Server to grab credentials from the Security Account Manager (SAM) database and Active Directory (AD)

After running these commands, the co-opted DebugView tool connected to multiple attacker-controlled domains, likely to exfiltrate stolen credentials.

As the affected organizations worked to evict BISMUTH from their networks, Microsoft security researchers saw continued activity involving lateral movement to other devices, credential dumping, and planting of multiple persistence methods. This highlights the complexity of responding to a full-blown intrusion and the significance of taking quick action to resolve alerts that flag initial stages of an attack.

Building organizational resilience against attacks that blend in

BISMUTH attacks put strong emphasis on hiding in plain sight by blending in with normal network activity or common threats that attackers anticipate will get low-priority attention. The combination of social engineering and use of legitimate applications to sideload malicious DLLs entail multiple layers of protection focused on stopping threats at the earliest possible stage and mitigating the progression of attacks if they manage to slip through. Here are mitigation recommendations that organizations can implement to limit exposure:

Limit the attack surface that attackers can leverage for initial access:

- Educate end users about protecting personal and business information in social media, filtering unsolicited communication, identifying lures in spear-phishing email, and reporting of reconnaissance attempts and other suspicious activity.
- Configure Office 365 email filtering settings to ensure blocking of phishing & spoofed emails, spam, and emails with malware. Set Office 365 to recheck links on click and delete sent mail to benefit from newly acquired threat intelligence.
- Turn on attack surface reduction rules, including rules that can block advanced macro activity, executable content, process creation, and process injection initiated by Office applications.
- Disallow macros or allow only macros from trusted locations. See the latest security baselines for Office and Office 365.
- Check perimeter firewall and proxy to restrict servers from making arbitrary connections to the internet to browse or download files. Such restrictions help inhibit malware downloads and command-and-control activity.

Build credential hygiene to reduce risk during discovery stage:

- Enforce strong, randomized local administrator passwords. Use tools like LAPS.
- Practice the principle of least-privilege and maintain credential hygiene. Avoid the use of domain-wide, admin-level service accounts.
- Require multi-factor authentication through Windows Hello.

Stop attack sprawl and contain attacker movement:

- Turn on cloud-delivered protection and automatic sample submission on Microsoft Defender Antivirus. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats.
- Turn on tamper protection features to prevent attackers from stopping security services.
- Monitor for clearing of event logs. Windows generates security event ID 1102 when this occurs.
- Determine where highly privileged accounts are logging on and exposing credentials. Monitor and investigate logon events (event ID 4624) for logon type attributes. Highly privileged accounts should not be present on workstations.
- Utilize the Microsoft Defender Firewall, intrusion prevention devices, and your network firewall to prevent RPC and SMB communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.

To better defend organizations against attacks that do everything to blend in once they gain access to a network, organizations can build defenses for preventing and blocking attacks at the initial access stage. Microsoft Defender for Office 365 provides defense capabilities that protect organizations from threats like credential phishing, business email compromise, and cyberattacks that begin with spear-phishing emails. Safe attachments and Safe links provide real-time protection using a combination of detonation, automated analysis, and machine learning, which are especially useful for highly targeted, specially crafted emails. Campaign views show the complete picture of email campaigns, including timelines, sending patterns, impact to the organization, and details like IP addresses, senders, URLs.

The broader Microsoft 365 Defender presents cross-domain threat intelligence and actionable information in consolidated incidents view, empowering security operations teams to comprehensively respond to attacks. For critical threats like BISMUTH campaigns, Microsoft researchers publish threat analytics reports that contain technical details, detection info, and mitigation status. Investigation tools like advanced hunting allow security teams to perform additional inspection of the environment for related or similar threats. Threat and vulnerability management data show mitigation recommendations, including enabling relevant attack surface reduction rules, that organizations can take to reduce risks.

These industry-leading capabilities in Microsoft 365 Defender are backed by Microsoft's network of researchers and security experts who monitor the threat landscape and track threat actors like BISMUTH. Through Microsoft 365 Defender, we transform threat intelligence into protections and rich investigation tools that organizations can use to build organizational resilience. Learn how you can stop attacks through automated, cross-domain security and built-in AI with Microsoft Defender 365.

Microsoft 365 Defender Threat Intelligence Team

with Microsoft Threat Intelligence Center (MSTIC)

MITRE ATT&CK techniques observed

Initial access

001 Phishing: Spearphishing Attachment| Emails containing malicious Word documents with specific lure themes and subject lines for each target

Execution

- 002 System Services: Service Execution| Use of Service Control Manager (*services.exe*) to launch Sysinternals *dbgview.exe*
- 001 Command and Scripting Interpreter: PowerShell| Use of PowerShell to run cmdlets used for data exfiltration and lateral movement

Persistence

T1053 Scheduled Task/Job| Scheduled task to execute payload every 60 minutes

Privilege escalation

002/003 Valid Accounts: Local and Domains Accounts| Credentials stolen for privilege escalation using Mimikatz

Defense evasion

Credential access

T1003Credential Dumping | Use of Mimikatz to dump credentials

Discovery

Collection

001 Data Staging: Local Data Staging| Storing harvested credentials and user/group information in a local CSV file

Data exfiltration

T1041 Exfiltration Over C2 Channel| Data exfiltration to a C2 server established in the compromised network