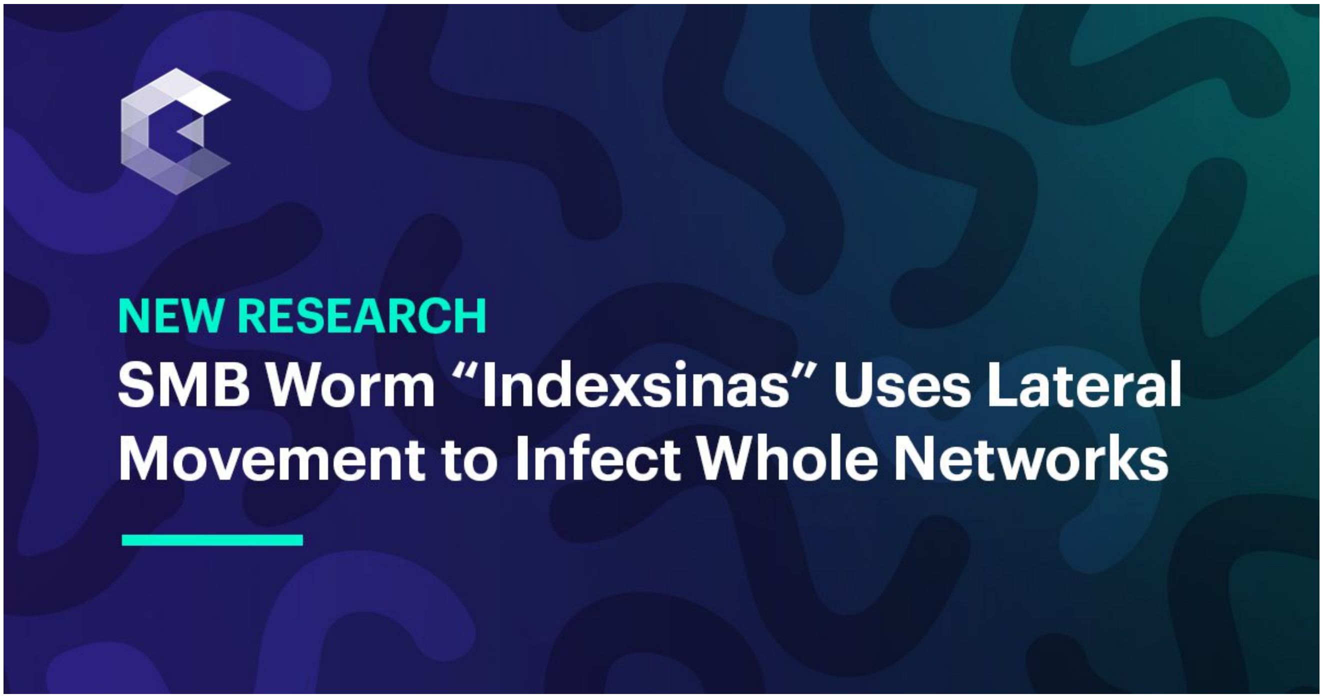
SMB Worm “Indexsinas” Uses Lateral Movement to Infect Whole Networks

guardicore.com/labs/smb-worm-indexsinas/


NEW RESEARCH
SMB Worm “Indexsinas” Uses Lateral Movement to Infect Whole Networks

Executive Summary

- Guardicore reveals new details in the Indexsinas SMB worm, also dubbed NSABuffMiner.
- The attack campaign has been active since 2019 and is still under operation and maintenance today.
- Targeted devices are SMB servers vulnerable to EternalBlue (MS17-010). According to Shodan, there are more than 1.2 million internet-facing SMB servers today.
- The attack makes vast use of the Equation Group exploit kit, which includes EternalBlue exploit as well as the DoublePulsar backdoor.
- Victims include organizations in the healthcare, hospitality, education and telecommunications sectors.

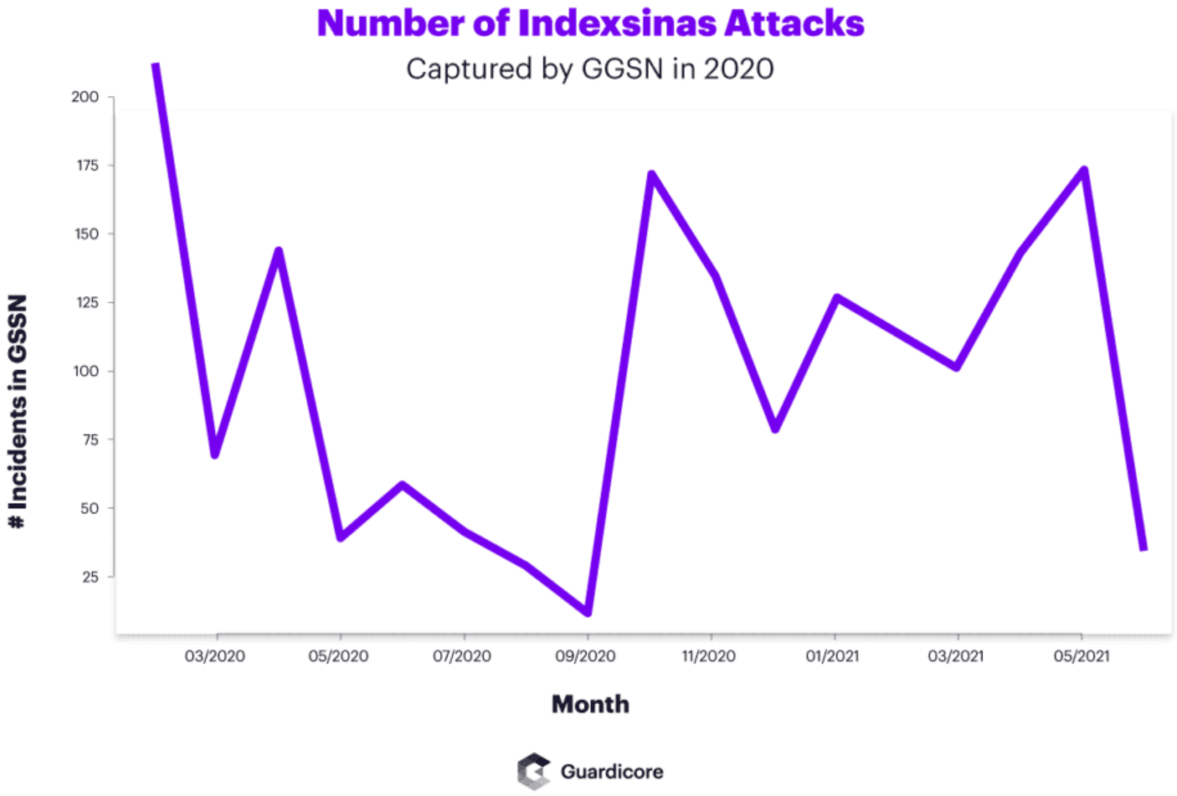
Guardicore Labs published a Github repository with all IOCs for this campaign as well as a detection tool in Powershell.

Guardicore Labs exposes new details of a massive attack campaign dubbed Indexsinas (also known as “NSABuffMiner”) which breaches networks through SMB servers and makes aggressive use of lateral movement to propagate. The attack campaign targets Windows servers vulnerable to EternalBlue (MS17-010) and still infects machines worldwide.

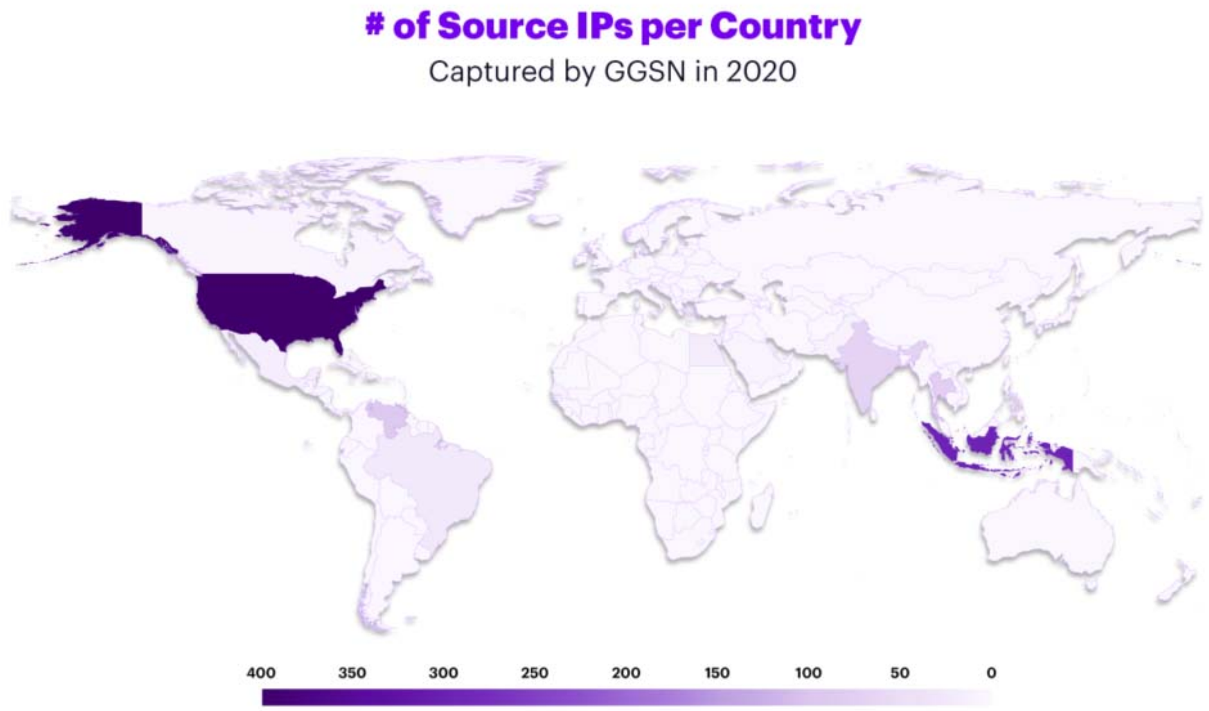
Propagation is achieved through the combination of an open source port scanner and three Equation Group exploits – EternalBlue, DoublePulsar and EternalRomance. These exploits are used to breach new victim machines, obtain privileged access, and install backdoors. These exploits appear to still be highly successful despite being made public four years ago after their first occurrence in the WannaCry and NotPetya cyberattacks. Indexsinas proves that networks today are vulnerable to even non-targeted, opportunistic attack campaigns.

Attack Scope

The Indexsinas campaign started attacking Guardicore Global Sensors Network (GGSN) at the beginning of 2019 and is still active today. Guardicore's sensors have recorded over 2,000 attacks since we began tracking the campaign.



The attacks originated from over 1,300 different sources, with each machine responsible for only a few attack incidents. Source IPs – which are likely to be victims of the attacks themselves – are mostly located in the U.S., Vietnam and India. Analysis of these IPs demonstrate that various sectors were infected by Indexsinas including hotels, universities, medical centers, government agencies and telecommunication companies.



# of Source IPs per Country

Captured by GGSN in 2020

Dark areas represent a higher number of source IPs

The Indexsinas attackers are careful and calculated. The campaign has been running for years with the same command-and-control domain, hosted in South Korea. The C2 server is highly protected, patched and exposes no redundant ports to the internet. The attackers use a private mining pool for their cryptomining operations, which prevents anyone from accessing their wallets' statistics.

Attack Flow

The attack flow consists of many batch scripts, executable payloads, downloaders, services and scheduled tasks. A prominent characteristic of the campaign is its competitiveness; it terminates processes related to other attack campaigns, deletes their file system residues and stops services created by other attack groups. It also attempts to evade detection by killing programs related to process monitoring and analysis. In addition, it makes sure to delete its own files immediately after execution.

Breach and the 1st Stage Downloader

The attack begins when a machine is breached through RPC or SMB servers, using the NSA's exploitation tools. These exploits run code in the victim's kernel and are capable of injecting payloads to user-mode processes using asynchronous procedure calls (APCs). Indexsinas uses the exploits to inject code to either *explorer.exe* or *lsass.exe*. The injected payloads – *EternalBlue.dll* for 32-bit and *DoublePulsar.dll* for 64-bit – download three executable files from the main C2 server, as detailed in the table below.

Files Downloaded at Stage #1

32-bit	**64-bit**
c64.exe	services.exe
iexplore.exe	
86.exe	64.exe

Persistence, Remote Access & C2 Reporting [86.exe, 64.exe]

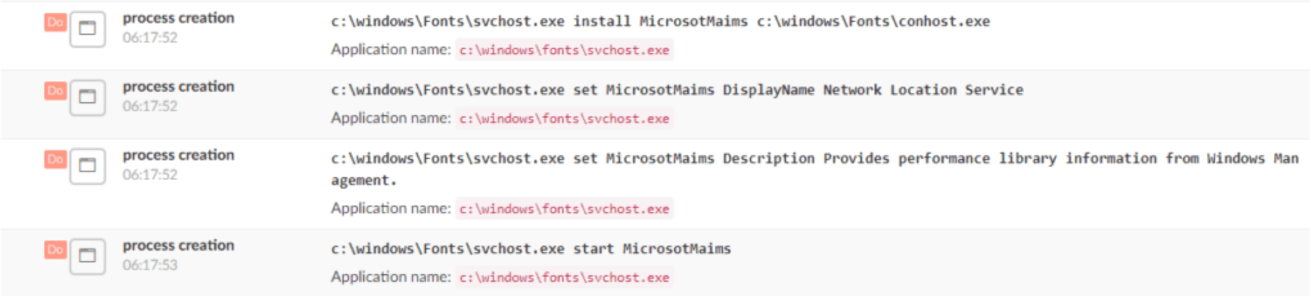
The *86.exe* and *64.exe* files contain a whole, reversed DLL, a Portable Executable file turned upside down, with “ZM” at the end (instead of “MZ” at the beginning). This DLL is a remote access tool (RAT), a version of Gh0stCringe. It is dropped to a random path and loaded into memory. Then, two of its exported functions are called – *Install* and *MainThread*. The first installs the RAT by creating a service under *svchost*, namely, it creates a registry key for the new service with *svchost.exe* as its executable and uses the path to the DLL as the *ServiceDLL* parameter. The second function performs the core functionality. It waits for commands from the C2 and reports machine information to it – computer name, malware group ID, installation date and CPU technical specs. The tool has various capabilities; it can download and execute additional modules, install them as services, and interact with the user by opening message boxes and presenting URLs in Internet Explorer.

Remote Access Tool (DLL) Exported Functions

Export Name	Description
Install	Installs a service whose image is the DLL itself. The service runs under *svchost*.
MainThread	Performs C2 communication; sends machine information and receives C2 commands.
ServiceMain	Gain elevated privileges by obtaining the SYSTEM user’s token.
Uninstall	Remove the malware from the system completely.
DllUpdate	Updates the DLL to a newer version.

Cryptominer [iexplore.exe, services.exe]

The *iexplore.exe* and *services.exe* files install two services using a tool masqueraded as *svchost.exe*. The first service – *MicrosotMaims* – is responsible for dropping a cryptominer through an additional file named *conhost.exe*.



```
Do  process creation   c:\windows\Fonts\svchost.exe install MicrosotMaims c:\windows\Fonts\conhost.exe
    06:17:52           Application name: c:\windows\fonts\svchost.exe

Do  process creation   c:\windows\Fonts\svchost.exe set MicrosotMaims DisplayName Network Location Service
    06:17:52           Application name: c:\windows\fonts\svchost.exe

Do  process creation   c:\windows\Fonts\svchost.exe set MicrosotMaims Description Provides performance library information from Windows Man
    06:17:52           agement.
                       Application name: c:\windows\fonts\svchost.exe

Do  process creation   c:\windows\Fonts\svchost.exe start MicrosotMaims
    06:17:53           Application name: c:\windows\fonts\svchost.exe
```

Guardicore Centra shows the creation of a new service MicrosotMais

The second – *MicrosotMaim* – simply runs the cryptominer module. The miner process is named *d1lhots.exe;* it is compiled from XMRig, mines Monero and is executed via the command line below.

```
d1lhots -o stratum+tcp://a.ccmd.website:1188 -u Bing1 -k –max-cpu-usage=50 –donate-
level=1 -r3 –asm=AUTO –print-time=3 –nicehash
```

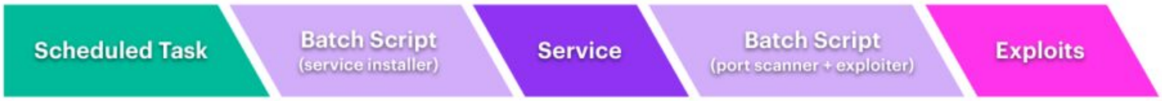
iexplore.exe drops two additional scripts. The first – *chosts.bat* – is a batch script which modifies the local firewall rules using *ipsec* and blocks any incoming traffic to SMB and RPC ports (135, 137, 138, 139 and 445). The second script – *tem.vbs* – is used to delete both *iexplore.exe* and itself.

Propagation [c64.exe]

Another payload which is downloaded as part of the 1st stage is *c64.exe*, which in turn drops two files. The first is *xfsxdel~.exe* and is only used to delete *c64.exe* from disk. The second is *ctfmon.exe* – the propagation tool.

ctfmon.exe is responsible for finding potential victims and exploiting them using Equation Group's tools – and it does that extremely thoroughly. It uses exploits for both 32-bit and 64-bit machines and scans both RPC (TCP 139) and SMB (TCP 445) ports. Moreover, it tries to move laterally within the organizational network as well as spread across the internet.

ctfmon.exe executes a batch script *same.bat*. This script initiates two flows: one for lateral movement within the network, and the other for spreading on the internet. The two flows are similar in their sequence: A daily scheduled task runs a batch script, which installs a service. The service runs another batch script which performs the port scanning and exploitation. The batch scripts in these flows also uninstall competitors' services, terminate their processes and delete their files. In addition, they clean old Indexsinas traces.



General Propagation Scheme

1. **Lateral Movement.** The scheduled task *At2* runs daily. It executes a batch script – *wai.bat* – which installs a service called *MicrosoftMssql*. The service runs *bat.bat*, which scans known private IP ranges.
2. **Internet Worm.** The scheduled task *At1* runs daily. It executes a batch script – *nei.bat* – which installs a service called *MicrosoftMysql*. The service runs *cmd.bat*, which scans the class C subnet of the victim's public IP address.

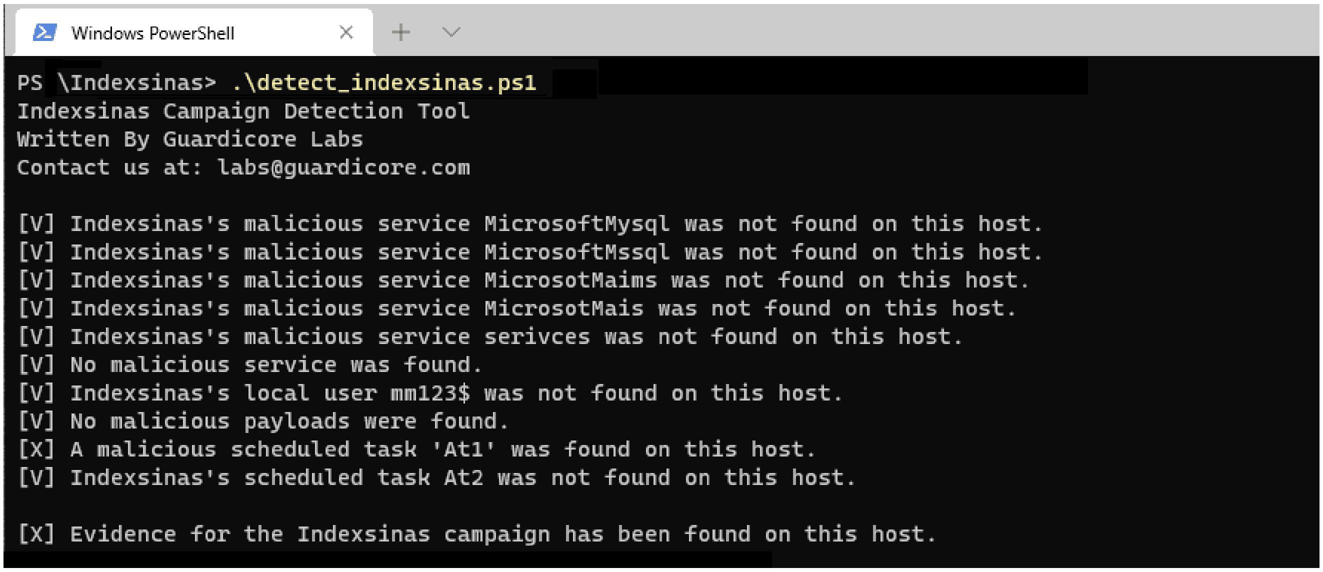
Indexsinas makes use of an open-source port scanner called ***s*** that is compiled into an executable file titled *taskhost.exe*. The scanner outputs a list of servers whose SMB ports are open in a file called *Results.txt*. Then, each IP in that list is attacked using Equation Group's exploits.

Upon successful exploitation, DoublePulsar.dll (for 64-bit) or EternalBlue.dll (for 32-bit) are injected into the victim machine's kernel and the attack flow starts all over again on the newly-infected machine.

Detection and Prevention

Detection

Guardicore Labs publishes a detection tool in PowerShell which identifies malicious indicators of compromise on a Windows machine. Execute this script from a command line prompt to see whether the system is infected or not. Detailed instructions can be found in Guardicore Labs' Github repository.



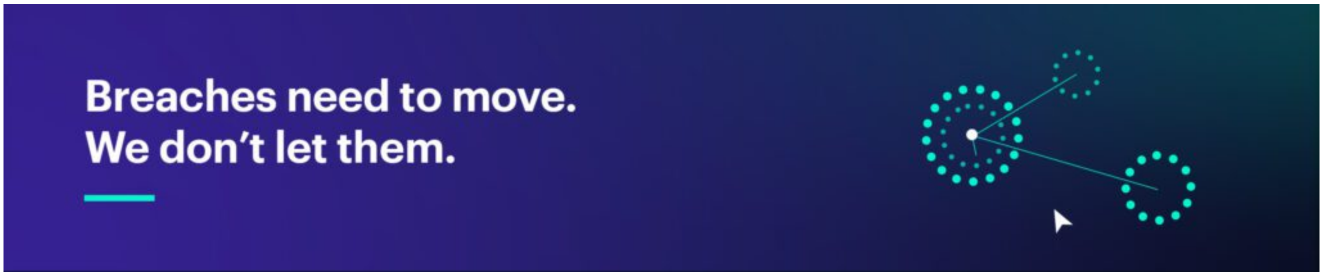
```
PS \Indexsinas> .\detect_indexsinas.ps1
Indexsinas Campaign Detection Tool
Written By Guardicore Labs
Contact us at: labs@guardicore.com

[V] Indexsinas's malicious service MicrosoftMysql was not found on this host.
[V] Indexsinas's malicious service MicrosoftMssql was not found on this host.
[V] Indexsinas's malicious service MicrosotMaims was not found on this host.
[V] Indexsinas's malicious service MicrosotMais was not found on this host.
[V] Indexsinas's malicious service serivces was not found on this host.
[V] No malicious service was found.
[V] Indexsinas's local user mm123$ was not found on this host.
[V] No malicious payloads were found.
[X] A malicious scheduled task 'At1' was found on this host.
[V] Indexsinas's scheduled task At2 was not found on this host.

[X] Evidence for the Indexsinas campaign has been found on this host.
```

Guardicore Labs detection tool for Indexsinas executed and reports infection

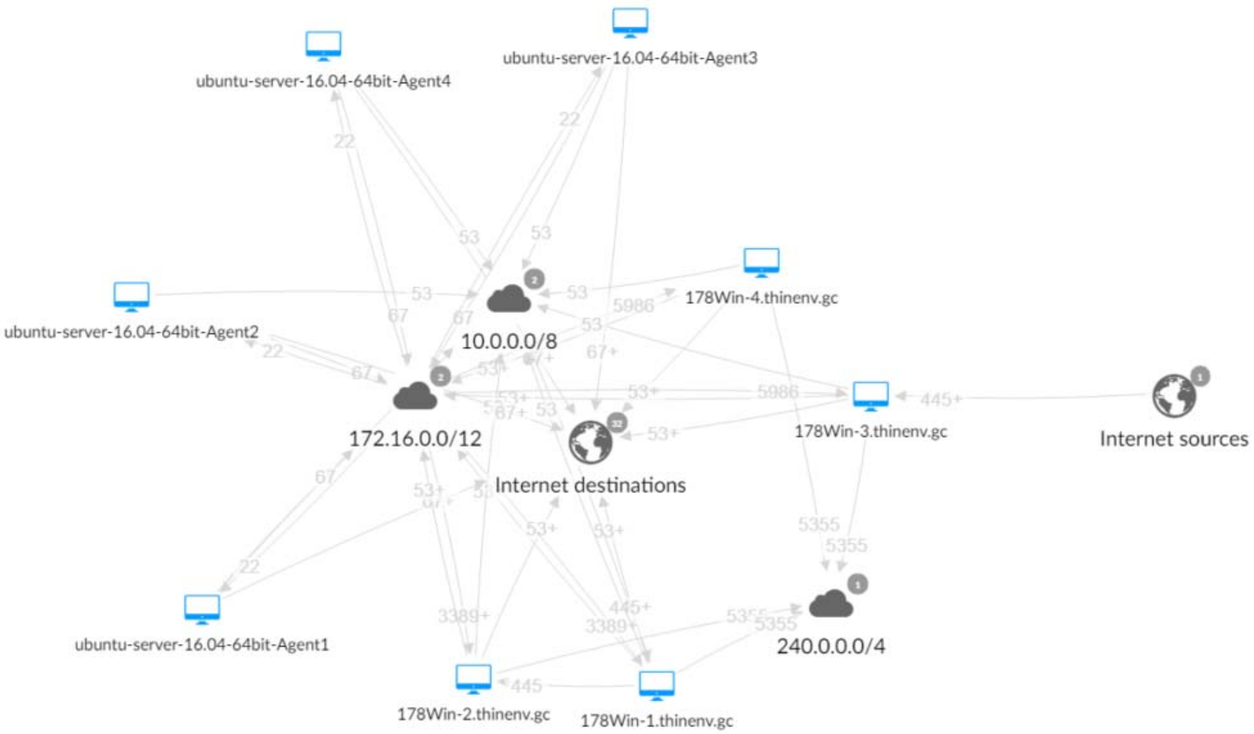
Prevention with Visibility and Segmentation

Indexsinas and other attack campaigns leverage vulnerable SMB servers to breach networks and move laterally inside them. There are more than 1 million SMB servers accessible to anyone on the internet, and many of them still vulnerable to MS-17010; this is exactly what makes Indexsinas and similar attack campaigns profitable.

The keys to recognizing vulnerable entry points with your organization and preventing attacks from propagating within the network are **visibility** and **segmentation**.



It is crucial that network administrators, IT teams and security personnel be able to easily identify assets and the services they run. Specifically, it should be easy to spot internet-facing servers, SMB included.

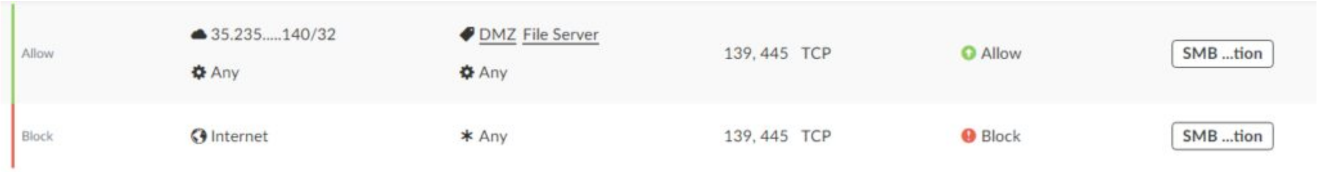


Guardicore Centra visibility map shows internet-facing SMB servers and connections they receive

With visibility in place, network admins would want to limit the access from and to different assets and the network services they expose.

The following are examples of policy rules which can protect your organization's SMB servers:

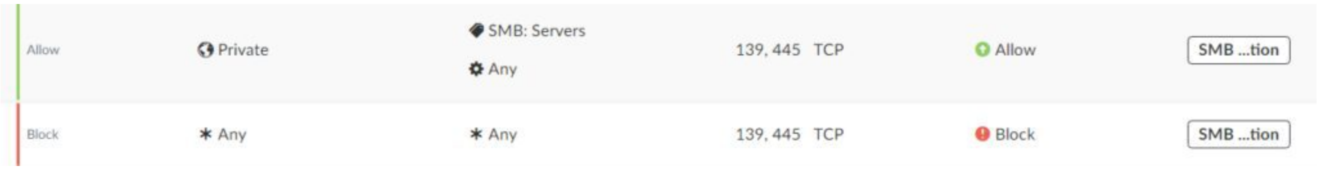
> Access from the internet over SMB is not allowed, except from certain authorized IP addresses to a file server in the DMZ



Allow	35.235.....140/32 ⚙ Any	DMZ File Server ⚙ Any	139, 445 TCP	Allow	SMB ...tion
Block	Internet	* Any	139, 445 TCP	Block	SMB ...tion

Guardicore Centra rule to allow only certain IP addresses to access internet-facing file servers in the organization

> SMB traffic inside the network is blocked, except for Domain Controllers and SMB file servers



Allow	Private	SMB: Servers ⚙ Any	139, 445 TCP	Allow	SMB ...tion
Block	* Any	* Any	139, 445 TCP	Block	SMB ...tion

Guardicore Centra rule to allow SMB traffic inside the network only to file servers and domain controllers

The threat of lateral movement is as worrying as the threat of ransomware

On June 2nd, the U.S. White House sent an open letter to corporate executives and business leaders in the private sector, urging them to take action and defend their organizations from ransomware. One paragraph stands out in this memo as it addresses the data center's network itself, clearly stating the importance of segmenting corporate networks. Network segmentation not only prevents an attacker from moving laterally and reaching strategic assets and crown jewels in the network; it also helps minimize damage (reduce the blast radius) by creating boundaries between servers in the network and limiting the network traffic between them.

> **Segment your networks**: There's been a recent shift in ransomware attacks – from stealing data to disrupting operations. It's critically important that your corporate business functions and manufacturing/production operations are separated and that you carefully filter and limit internet access to operational networks, identify links between these networks and develop workarounds or manual controls to ensure ICS networks can be isolated and continue operating if your corporate network is compromised. Regularly test contingency plans such as manual controls so that safety critical functions can be maintained during a cyber incident.

But don't be misled by the title mentioning only the "threat of ransomware". Lateral movement inside a compromised network can be used to drop any type of payload – be it ransomware, remote access tools, backdoors and cryptominers. Lateral movement is the real threat whereas ransomware is only one motive implementing it. In the case of Indexsinas, lateral movement is used to infect as many machines as possible with a remote access tool and a cryptominer. Network segmentation is crucial in preventing such campaigns from spreading and disrupting business operations.

Indicators of Compromise

Please see the full lists of IOCs in our Github repository.

Domains

- 1.indexsinas.me
- 2.indexsinas.me
- a.ccmd.website

Mutexes

- ipip.website

- dllhost.website

Service Names

- MicrosotMaims
- MicrosotMaim
- MicrosoftMysql
- MicrosoftMssql
- Services

Scheduled Tasks

- At1
- At2