



SDBBot Malware threat to US Healthcare Organizations

Executive Summary

The Australian Cyber Security Center (ACSC) published an alert on November 12 related to two malware variants – Clop (ransomware) and SDBBot, a remote access trojan (RAT), noting that they together have recently been used by one or more cybercriminal groups to target Australian healthcare organizations. HC3 has historically observed the targeting of healthcare organizations often crossing international borders. Furthermore, the threat actor believed to utilize Clop and SDBBot has targeted American healthcare previously, including a campaign using the Coronavirus as a phishing theme. As such, HC3 believes the US healthcare community are at an elevated threat of being targeted by both Clop and SDBBot. This report will analyze and recommend defensive measures for SDBBot and will be released along with a companion report addressing Clop ransomware.

Analysis

On November 12, 2020, the Australian Cyber Security Center (ACSC) [published an alert on Clop ransomware and SDBBot](#), a RAT, which has been targeting the Australian healthcare industry. It has a common design framework and functionality which we will review in this report. SDBBot was first discovered in 2019, identified by AhnLab in their [Q3 Security Emergency-response Center report](#) as well as by ProofPoint in a [malicious activity report](#). is written in C++ and consists of three components – an installer for persistence, a dropper which delivers additional malware or ransomware, and the RAT functionality. The installer stores the RAT component in the registry and establishes persistence for the loader component. Some versions are known to use the filename SdbInstallerDII[.]dll for the installer. For at least some versions, a registry value is created at “\SOFTWARE\Microsoft\

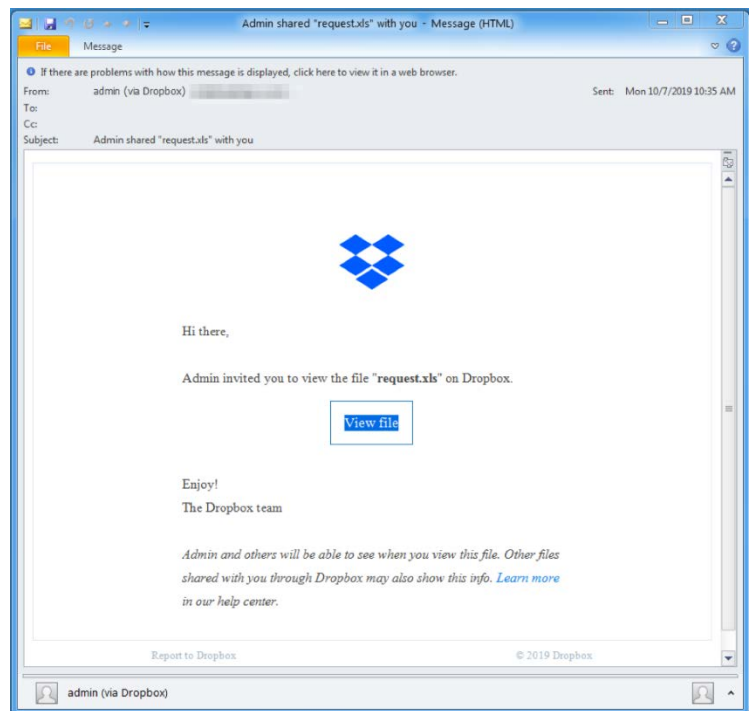


Figure 1: Malspam with malicious .xls attachment courtesy of Proofpoint



The threat actor that deploys SDBBot is known by a number of labels including TA505 (Proofpoint), Graceful Spider (CrowdStrike), Gold Ever, green (SecureWorks), TEMP.Warlock (FireEye), ATK 103 (Thales), SectorJ04 (ThreatRecon), Hive0065 (IBM), and Chimborazo (Microsoft). They are affiliated with the various cybercriminal gangs given the spider label by CrowdStrike, most prominently, Monty Spider, Mummy Spider, Ratopak Spider, Indrik Spider, Doppel Spider and Dungeon Spider. They are a financially-motivated cybercriminal group widely believed to operate out of Russia and known to target healthcare organizations, in addition to education finance, hospitality and retail. They also are known to frequently shift their tactics, techniques and procedures (TTPs) and leverage a variety of malware variants. TA505 is observed to have

followed the general pattern of many cybercriminal groups who, since 2018, have increasingly leveraged backdoors, downloaders, information gathering weapons, remote access trojans and other malware types as first stage attacks and followed it with second stage ransomware at times, instead of deploying ransomware as the only stage of their attack. SDBBot is one of the many cyber threat actors that has [leveraged COVID19-themed phishing campaigns](#). In addition to spear-phishing, TA505 has been known to use many other

Domains reported by X-Force	Domains reported by Proofpoint	Domains reported by ZeroFOX
drm-server-booking[.]com	news-server-drm-google[.]com	office-en-service[.]com
microsoft-live-us[.]com	update365-office-ens[.]com	googledrive-download[.]com
dl1.sync-share[.]com	office365-update-en[.]com	dl1.syncdownloading[.]com

Figure 2: TA505 phishing domains as reported by IBM X-Force IRIS and others

tactics, techniques and procedures (TTPs) including the use of macro-enabled documents, droppers containing embedded dynamic-link libraries (DLLs), installer components, legitimate cloud hosting services for malware distribution as well as spoofing legitimate services such as Microsoft and Google the use of command and control domains that follow a pattern of naming convention and structure (see diagram on this page).

In addition to SDBBot, they are also known to utilize Amadey, AndroMut, Bart, CryptoLocker, CryptoMix, Dridex, Dudear, EmailStealer, FlawedAmmy, FlawedGrace, FlowerPippi, GameOver Zeus, Gelup, Get2, GlobelImposter, Jaff, Kegotip, Locky, MINEBRIDGE, Neutrino, Philadelphia, Pony, RockLoader, RMS, SDBbot, ServHelper, Shifu, Snatch, TinyMet and Zeus. They are also known to use administrative tools resident on a victim system known as “living off the land”. Finally, its worth noting that TA505 likely has a connection to FIN11. This connection may mean they are separate cybercriminal groups that collaborate, or they are separate cybercriminal groups with overlapping membership or the remote possibility that they are the same cybercriminal group. Most likely, [FIN11 is a spin-off group from TA505](#). FIN11 is known to operate CLOP ransomware among other malware and ransomware variants.

TA505’s use of malspam/phishing is prolific. According to [one analytic company](#), they are. “responsible for the largest malicious spam campaigns we have ever observed, distributing instances of the Dridex banking Trojan, Locky ransomware, Jaff ransomware, The Trick banking Trojan, and several others in very high volumes. TA505 is reported to have infrastructure overlap with Buhtrap and Ratopak Spider. One analytic company found relationships between TA505 and other cyber threat groups such as Silence and Contract Crew.

SDBBot was [first identified in September, 2019 as part of a greater phishing campaign](#) that was delivering Get2 as the first stage malware, which in turn dropped SDBBot, in addition to other payloads. It was also observed [being dropped in the spring of 2020](#) with COVID19-themed phishing attacks. Finally, as previously mentioned, the Australian government has recently warned their healthcare sector of SDBBot attacks.



The below table shows SDBBot mapped against the MITRE ATT&CK Framework. The most updated version can be found on the MITRE website at: <https://attack.mitre.org/software/S0461/>

DOMAIN	ID	NAME	USE
Enterprise	T1547 0	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	SDBot has the ability to add a value to the Registry Run key to establish persistence if it detects it is running with regular user privilege.
Enterprise	T1059 0	Command and Scripting Interpreter: Windows Command Shell	SDBot has the ability to use the command shell to execute commands on a compromised host.
Enterprise	T1005	Data from Local System	SDBot has the ability to access the file system on a compromised host.
Enterprise	T1140	Deobfuscate/Decode Files or Information	SDBot has the ability to decrypt and decompress its payload to enable code execution.
Enterprise	T1546 0.01	Event Triggered Execution: Image File Execution Options Injection	SDBot has the ability to use image file execution options for persistence if it detects it is running with admin privileges on a Windows version newer than Windows 7.
	0.01	Event Triggered Execution: Application Shimming	SDBot has the ability to use application shimming for persistence if it detects it is running as admin on Windows XP or 7, by creating a shim database to patch services.exe.
Enterprise	T1083	File and Directory Discovery	SDBot has the ability to get directory listings or drive information on a compromised host.
Enterprise	T1070	Indicator Removal on Host	SDBot has the ability to clean up and remove data structures from a compromised host.[1]
	0	File Deletion	SDBot has the ability to delete files from a compromised host.
Enterprise	T1105	Ingress Tool Transfer	SDBot has the ability to download a DLL from C2 to a compromised host.
Enterprise	T1095	Non-Application Layer Protocol	SDBot has the ability to communicate with C2 with TCP over port 443.
Enterprise	T1027	Obfuscated Files or Information	SDBot has the ability to XOR the strings for its installer component with a hardcoded 128 byte key.
	0	Software Packing	SDBot has used a packed installer file.
Enterprise	T1055 0	Process Injection: Dynamic-link Library Injection	SDBot has the ability to inject a downloaded DLL into a newly created rundll32.exe process.
Enterprise	T1090	Proxy	SDBot has the ability to use port forwarding to establish a proxy between a target host and C2.
Enterprise	T1021 0	Remote Services: Remote Desktop Protocol	SDBot has the ability to use RDP to connect to victim's machines.
Enterprise	T1082	System Information Discovery	SDBot has the ability to identify the OS version, country code, and computer name.
Enterprise	T1016	System Network Configuration Discovery	SDBot has the ability to determine the domain name and whether a proxy is configured on a compromised host.
Enterprise	T1033	System Owner/User Discovery	SDBot has the ability to identify the user on a compromised host.
Enterprise	T1125	Video Capture	SDBot has the ability to record video on a compromised host.



Detection, mitigation and remediation

Preventing the initial attack vector is the optimal outcome for any cyberattack. With SDBBot, because malspam/phishing is the typical approach by an attacker, preventing phishing attacks is critical. This can be done with the following actions:

- **Security awareness training** – Ensuring your workforce does not interact with malicious e-mails with periodic, iterative awareness training
- **E-mail gateway filtering** – Deploying, operating and maintaining e-mail gateway filtering software at your enterprise e-mail server(s)
- **Endpoint security** – Deploying, operating and maintaining endpoint security software to prevent malware from executing after a successful infection vector has executed
- **E-mail Marking** – Ensure emails originating from outside the organization are automatically marked before received.

Malware communicates across networks and the Internet in order to function, and in order to identify this, the following is recommended:

- **Intrusion Detection/SIEM tool usage** – Maintaining an intrusion detection capability which covers the entire information infrastructure including all network segments, endpoint systems and critical systems and servers is important to identifying malicious behavior and communications. Continuously monitor all available sources, including open source reporting and proprietary feeds, of indicators of compromise. Operationalize them in accordance with overall risk management posture. Some IOCs are listed below.
- **Whitelist authorized software** – Implement whitelisting technology to ensure only authorized software is allowed to execute. This can reduce the false positives making incident handlers more efficient.

Perimeter security is critical when defending against all cyber threats, and is certainly applicable to a good overall posture when preventing SBBot attacks.

- **Firewall maintenance** – Block suspicious IP addresses at the firewall; Keep firewall rules are updated
- **Patching** – Conduct system hardening to ensure proper configurations; Implement and maintain a patch management program to ensure new vulnerabilities are addressed shortly as they are periodically disclosed.
- **Disable vulnerable protocols** – Disable the use of SMBv1 and require at least SMBv2. Minimize or completely reduce the use of remote desktop protocol (RDP).

Indicators of compromise: There are many IOCs related to SDBBot available on the Internet. Only a very small sample of them are included below. may become “burned” – the attackers may adjust their TTPs, weapons and infrastructure rendering public IOCs obsolete. They can also bring obsolete IOCs back into use, so an organization should consider all possibilities. New IOCs are constantly being released and it is therefore critical to maintain situational awareness and be ever on the lookout for new IOCs to operationalize.

Additional indicators can be found at:

<https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader>



References

SDBBot Targeting Health Sector

<https://www.cyber.gov.au/acsc/view-all-content/alerts/sdbbot-targeting-health-sector>

Hackers publish ExecuPharm internal data after ransomware attack

<https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/>

A Few Cybercriminal Groups Claim to Be Easing the Grip

<https://securityboulevard.com/2020/06/covid-19-ruthless-ransomware-authors-attack-hospitals/>

TA505 Distributes New SDBbot Remote Access Trojan with Get2 Downloader

<https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader>

Event Triggered Execution: Application Shimming

<https://attack.mitre.org/techniques/T1546/011/>

AhnLab Q3 Security Emergency-response Center report

https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.96_ENG.pdf

Covid-19: Ruthless Ransomware Authors Attack Hospitals

<https://securityboulevard.com/2020/06/covid-19-ruthless-ransomware-authors-attack-hospitals/>

FIN11 Spun Out From TA505 Umbrella as Distinct Attack Group

<https://www.securityweek.com/fin11-spun-out-ta505-umbrella-distinct-attack-group>

TA505 Continues to Infect Networks With SDBbot RAT

<https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/>

TA505 Malware Threat Insights

<https://www.proofpoint.com/us/blog/threat-insight/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack>

TA505 Continues to Infect Networks With SDBbot RAT

<https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/>

TA505 Crime Gang Deploys SDBbot for Corporate Network Takeover

<https://threatpost.com/ta505-crime-gang-sdbbot-corporate-network-takeover/154779/>



FIN11 Cybercrime Gang Shifts Tactics to Double-Extortion Ransomware

<https://threatpost.com/fin11-gang-double-extortion-ransomware/160089/>

Australian government warns of possible ransomware attacks on health sector

<https://www.zdnet.com/article/australian-government-warns-of-possible-ransomware-attacks-on-health-sector/>

MITRE ATT&CK: TA505

<https://attack.mitre.org/groups/G0092/>

MITRE ATT&CK: SDBOT

<https://attack.mitre.org/software/S0461/>

Threat Actor Profile: TA505, From Dridex to GlobeImposter

<https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter>

TA505 shifts with the times

<https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times>

ServHelper and FlawedGrace - New malware introduced by TA505

<https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505>

Eager Beaver: A Short Overview of the Restless Threat Actor TA505

<https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546>

Development of the Activity of the TA505 Cybercriminal Group

<https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf>

TA505 returns with a new bag of tricks

<https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104>

SDBbot Unpacker

<https://github.com/Tera0017/SDBbot-Unpacker>

TA505's Box of Chocolate - On Hidden Gems packed with the TA505 Packer

<https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672>



CrowdStrike 202 Global Threat Report

<https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf>

Secureworks Threat Profiles: Gold Tahoe

<https://www.secureworks.com/research/threat-profiles/gold-tahoe>

HHS 405(d) Program

<https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf>