Health Sector Cybersecurity Coordination Center (HC3)

Analyst Note

September 8, 2020 **TLP: WHITE** **Report: 202009080830**

Maldocs used to Deliver Information Stealer

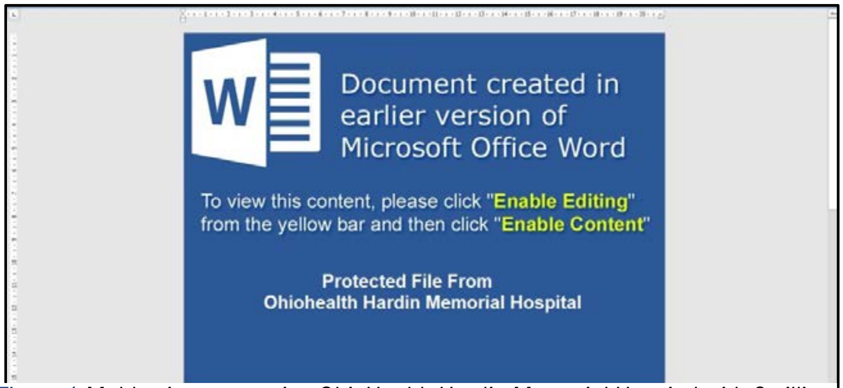
Executive Summary

In August 2020, security researchers identified a malicious email campaign impersonating a US hospital that was observed delivering a variety of information stealing trojans, including AgentTesla, Formbook, Matiex, and njRatAzorult. A recent uptick in detections submitted to VirusTotal suggests the actor may be ramping up their operations and the specific malicious documents (maldocs). creation technique detailed in this report is likely to be observed more in the wild. Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs) are included in the report.

Report

In July 2020, researchers at NVISO Labs (a European cybersecurity start-up located in Brussels, Belgium) detected a malicious email campaign leveraging a technique where the threat actors created macro-laden Excel workbooks. The actors likely used the EPPlus software instead of Microsoft Office, which often results in a lower detection rate compared to standard malicious documents).

The very first maldoc detected by the researchers was created on June 22, 2020. Since then, more than 200 malicious documents were found over a period of two months. According to NVISO, the actor has increased their activity in the last few weeks and the researchers discovered more than ten new malicious documents on some days.



Document created in earlier version of Microsoft Office Word

To view this content, please click "Enable Editing" from the yellow bar and then click "Enable Content"

Protected File From Ohiohealth Hardin Memorial Hospital

Figure 1 Maldoc impersonating OhioHealth Hardin Memorial Hospital with Cyrillic Word settings. Source: NVISO Labs.

The payloads observed before September 1, 2020 were predominantly information stealers. Information stealers, including Azorult, njRAT, AgentTesla, Formbook, and Matiex, are designed to harvest passwords from browsers, email clients, etc. The payloads stemming from these maldocs have evolved only slightly in terms of obfuscation and masquerading, indicating there is a likely a single actor behind the campaign.

In the six emails the researchers were able to retrieve, some recipients were in the medical equipment sector. One maldoc explicitly impersonated a healthcare entity, OhioHealth Hardin Memorial Hospital, as shown in Figure 1. The malicious Office Open XML Spreadsheet had Cyrillic word settings according to the researchers, indicating the threat actors are likely Russian-speaking. The maldoc also had a Korean language file name, implying the target of the campaign was likely Korean-speaking. While the template from the hospital may have been simply discovered on the web and consequently used by the threat actor, this surprising change in modus operandi does appear to align with the actor's constant evolution observed since the start of tracking, according to NVISO. The targeting seems rather limited for now, it is possible these first runs were intended for testing rather than a full-fledged campaign.

Xavier Mertens of SANS, recently published a blog post in which they analyzed some samples which were identified as AgentTesla. Mertens extracted and uploaded the VBA code from the maldocs related to the PowerShell technique used to download the next stage.

The second-stage payload for this campaign is downloaded from various websites via a malicious VBA code. Each second-stage executable created by its respective malicious document acts as dropper for the final payload. In order to thwart detection mechanisms such as antivirus solutions, a variety of obfuscation techniques (i.e. steganography) are leveraged. These obfuscation techniques are not advanced enough to hide the malicious intent. The infrastructure used by the threat actor appears to mainly leverage compromised websites.

Within the manually analyzed dataset of 30 distinct dictionary-based second stages, 19 unique final payloads were observed. From these, Azorult accounts for 50% of the variant's delivery (Figure 2). Other payloads include AgentTesla, Formbook, Matiex and njRat. Both Azorult and njRAT have a noticeable reusage rate.

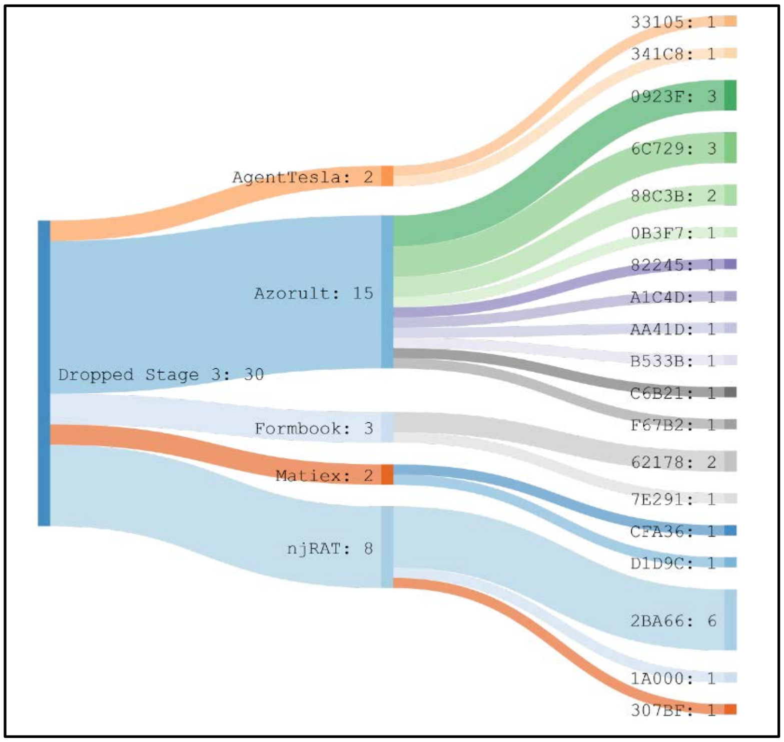


Figure 2 Dictionary-based payload classification and (re-)usage of samples with trimmed hashes for Epic Manchego campaign. Source. NVISO Labs

The malicious document impersonating OhioHealth Hardin Memorial Hospital has the following details:

Filename	새로운 주문 _2608.xlsm (Korean: New order _2608.xlsm)
MD5	551b5dd7aff4ee07f98d11aac910e174
SHA1	648b9c1615be047c36f017e398dca95febf6b4d9
SHA256	45cab564386a568a4569d66f6781c6d0b06a9561ae4ac362f0e76a8abfede7bb
File Size	5.77 KB (5911 bytes)
FireEye Detection	Trojan.GenericKD.43735448
Earliest Contents Modification	2020-06-22 14:01:46
Contacted URLS	hxxps://dc.services.visualstudio.com/v2/track hxxp://greenhillsrishikesh.com/nel.exe
Contacted IPs	185[.]136.167.228 (DE- Germany)

Analyst Comment

Most of the email sender domains in this campaign are from legitimate companies and it is possible the HPH organization in question was victim to business email compromise (BEC) or email spoofing. The impersonated healthcare entity most likely relates to OhioHealth Hardin Memorial Hospital (ohiohealth.com). While HC3 was unable to confirm whether the HPH entity was victim to BEC or email spoofing, below are some recommendations to mitigate that type of attack according to a previous HC3 briefing:

- Email warning banners for external senders and flags;
- Implement spoofing controls such as Sender Policy Framework (SPF), Domain-based Message

Authentication Reporting and Conformance (DMARC) and DomainKeys Identified Mail (DKIM) and fully configure for mail-enabled domains with hard fail and reject policies where applicable;

- Implement Two-Factor or Multi-Factor Authentication;
- Enforce strong password policies;
- Consider email security gateways for pre-delivery protection;
- Block macros to defend against malicious macros embedded in email attachments.

References

NVISO Labs, Epic Manchego – atypical maldoc delivery brings flurry of infostealers (1 September 2020)
https://blog.nviso.eu/2020/09/01/epic-manchego-atypical-maldoc-delivery-brings-flurry-of-infostealers/
SANS InfoSec Forums, Tracking A Malware Campaign Through VT (24 August 2020)
https://isc.sans.edu/forums/diary/Tracking+A+Malware+Campaign+Through+VT/26498/
HC3, Threat Briefing, TLP:WHITE Business Email Compromise in the Health Sector (9 July 2020)
https://www.hhs.gov/sites/default/files/business-email-compromise-in-the-health-sector.pdf
VirusTotal, Submission for Korean language maldoc (2 September 2020)
https://www.virustotal.com/gui/file/45cab564386a568a4569d66f6781c6d0b06a9561ae4ac362f0e76a8abfede7bb/detection
VirusTotal, Submission for maldoc with packing and invoice theme (1 September 2020)
https://www.virustotal.com/gui/file/0cffa3c199da1329d112028ae477e8b55c628bbf3cc9ad4693ec9c14d80f10f2/detection

Indicators of Compromise (IOCs) and Techniques

Epic Manchego IOCs: https://github.com/NVISO-BE/nviso-cti/tree/master/Epic_Manchego_IOC

ATT&CK IDS:
T1027 - Obfuscated Files or Information
T1036 - Masquerading
T1055 - Process Injection
T1140 - Deobfuscate/Decode Files or Information
T1204 - User Execution
T1497 - Virtualization/Sandbox Evasion
T1566 - Phishing

Campaign IOCs
45cab564386a568a4569d66f6781c6d0b06a9561ae4ac362f0e76a8abfede7bb
185.136.167.228
hxxps://dc.services.visualstudio.com/v2/track
hxxp://greenhillsrishikesh.com/nel.exe
greenhillsrishikesh.com
dc.services.visualstudio.com
3122ccb30fb346c6c6770ae26db7fabf870849078cbe0be173ee88ccf6512f98
fdb0bf9fcb5362739727fdf5e4e6021a071d30d476b738eab40d8d19f4733764
f2f3948a1b6f661f2a5169a86b7029166acd4b79d7abfd37fa2b646fe302bfd6
b368ba67eaf0445c8261c9b0e49b697ab90745ebae0ebe83f84f2e8a1090162a
092f00ac822a39696d81d85f12e4f65e6fe731e45bf6e4144b92ce876f6d314a
4d76fbaa21a01dab7ba72f545149d3a088039978a6276b9e6c26982684e56276

```
3277f17e4383c9f60e3c9d7af118f77133f3a90c392edc7bf7bbc4b6b2da00f7
f929220aadaff2334623be1cfddb3dc7080ab2288b19c2e05d19e29ead0222c0
563da000c83edc9e7aa8feb073e5680329b97127e5b26ff2866b1beaaf5217e6
da7da45664159ad2352a3582f7afc39d672bf5e20c9771eaca51d7c6eeb17a87
1b061c268a370892afa3d740d85850d0a987bcf0f064faa3e3e29902973d9b28
550ff784f20fa542d82aba5ae4b7f1774439226033e4ff0f0defc732a6d78c42
0cffa3c199da1329d112028ae477e8b55c628bbf3cc9ad4693ec9c14d80f10f2
45cab564386a568a4569d66f6781c6d0b06a9561ae4ac362f0e76a8abfede7bb
```