Compromised Servers & Fraud Accounts: Recent Hancitor Attacks

researchcenter.paloaltonetworks.com/2018/02/unit42-compromised-servers-fraud-accounts-recent-hancitor-attacks/

Vicky Ray, Brad Duncan February 7, 2018

By Vicky Ray and Brad Duncan

February 7, 2018 at 5:00 AM

Category: Malware, Unit 42

Tags: AutoFocus, Chanitor, DELoader, hancitor, Malspam, Pony, Torda, Vawtrak

This post is also available in: 日本語 (Japanese)

Unit 42 has been tracking malicious spam (malspam) pushing Hancitor malware during the past 2 years. Hancitor, also known as Chanitor or Tordal, is a macro-based malware spread through Microsoft Office documents distributed in malspam campaigns. Hancitor is designed to infect a victim's Microsoft Windows computer with additional malware, and the end result is most often a banking Trojan. But the impact of Hancitor malspam is fairly limited. On a default-configured Windows 10 host, the malware is easily detected by Microsoft's built-in Windows Defender anti-virus tool. Furthermore, many spam filters catch these emails before they get to their intended recipients.

Who is Hancitor effective against? An ideal target victim be someone running an outdated version of Windows like Windows 7 with anti-virus disabled. Such victims would also click through any warnings they encounter. Apparently, this target demographic is substantial enough that criminals behind Hancitor malspam continue to push their emails on a frequent basis.

While researchers have published many technical reports on Hancitor campaigns, their primary focus has been on the malware and its capabilities. But how does this type of attack with a limited base of victims remain profitable? Little has been published about how this campaign uses fraud accounts and the compromised infrastructure of legitimate businesses. Understanding the playbook used by these criminals is essential to understand why they continue to operate.

We continue to see several hundred examples of Hancitor malspam every month sent to a wide variety of recipients. The image below shows data extracted from our Autofocus threat intelligence platform. It provides high-level visibility on how frequently we've seen Hancitor malspam so far in 2017.

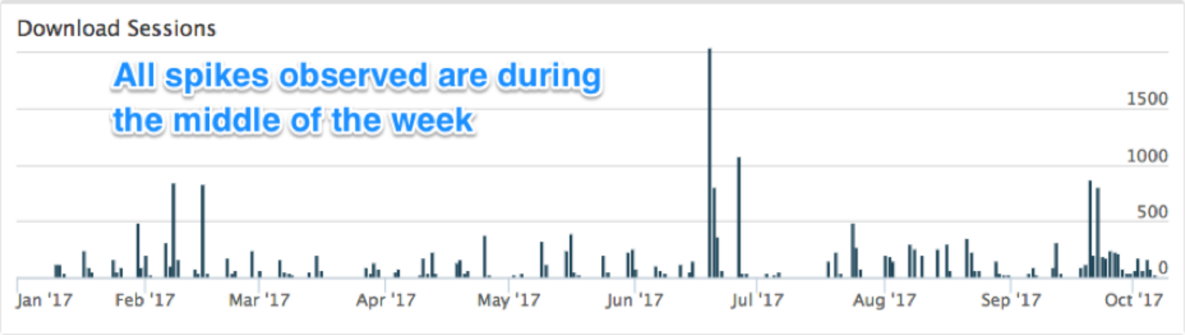


Figure 1: Timeline of Hancitor campaign activity since January 2017.

According to our Autofocus data, we can infer criminals behind this campaign follow a 5-day work week from Monday through Friday. Spikes in the email activity often occur in the middle of the week. This reflects a general pattern of productivity seen with most people who follow the same type of schedule.

Campaign History

In previous years, Hancitor malware was delivered as email attachments in malspam campaigns. Microsoft Word documents from this malspam downloaded other malware like Pony, Vawtrak, and DELoader as depicted in Figure 2.

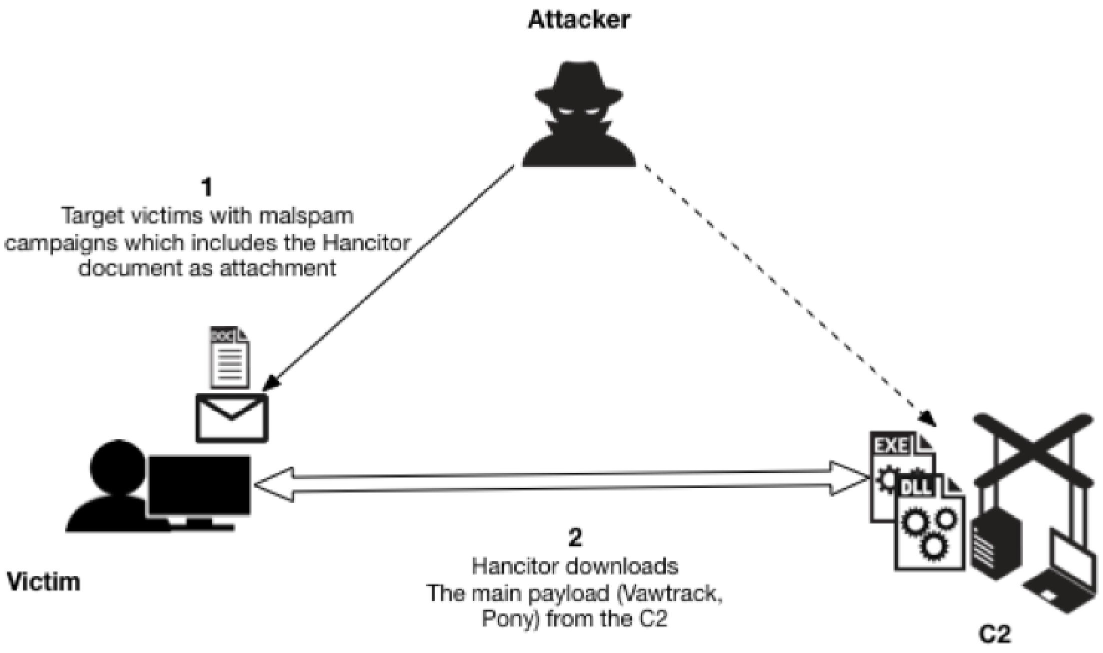

Attacker
1
Target victims with malspam campaigns which includes the Hancitor document as attachment
DOC
EXE
DLL
Victim
2
Hancitor downloads The main payload (Vawtrack, Pony) from the C2
C2

Figure 2: Hancitor downloaded as email attachments to targeted victims.

Hancitor Campaign Updates its Playbook

In the past, criminals have successfully infected victims using email attachments, but email filtering has improved in recent years. Most current enterprise-level security solutions now include a sharp focus on email attachments and can easily detect malicious documents and ultimately impact the success rate of the attackers' campaigns.

To further evade detection, since the end of 2016, actors behind Hancitor have added another step in the infection process. Instead of email attachments, a link in the email points to distribution servers hosting these Hancitor-base documents. Figure 3 outlines current campaign methods used to deliver Hancitor. This campaign continues to use distribution servers, indicating this technique has proven successful.

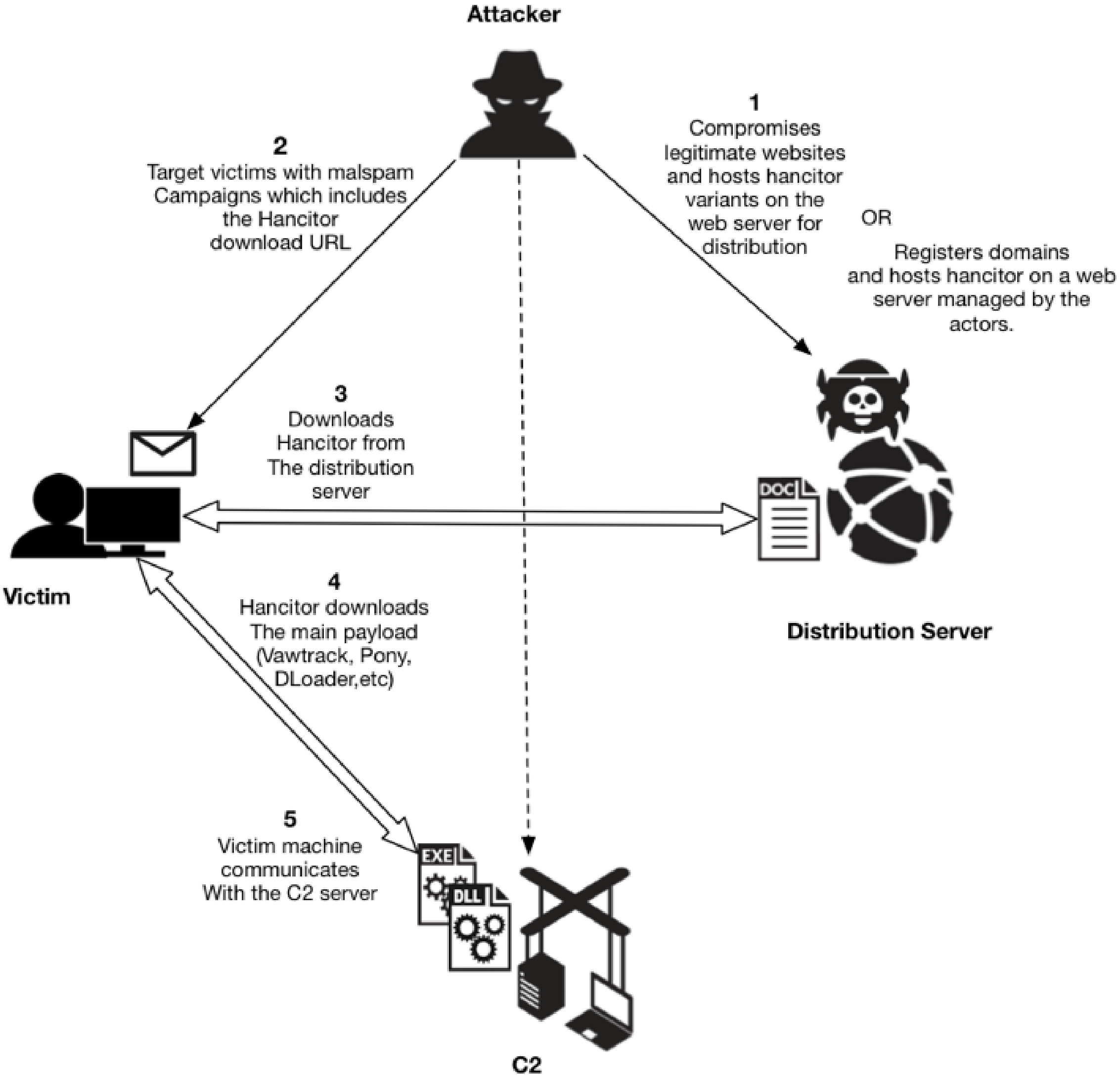
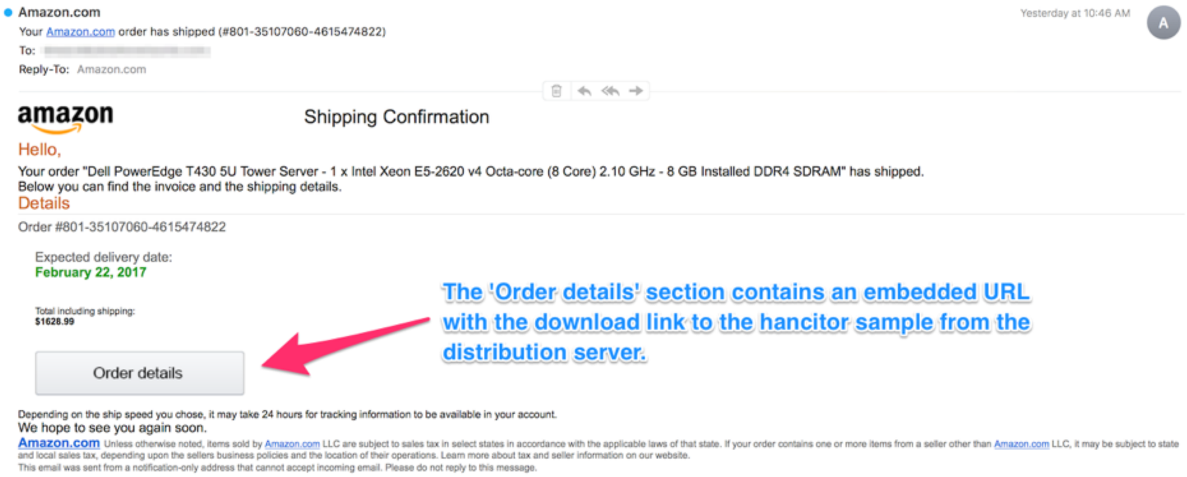

Attacker
1
Compromises legitimate websites and hosts hancitor variants on the web server for distribution
OR
Registers domains and hosts hancitor on a web server managed by the actors.
2
Target victims with malspam Campaigns which includes the Hancitor download URL
3
Downloads Hancitor from The distribution server
DOC
Victim
Distribution Server
4
Hancitor downloads The main payload (Vawtrack, Pony, DLoader,etc)
5
Victim machine communicates With the C2 server
EXE
DLL
C2

Figure 3: Current depiction of Hancitor delivery using distribution servers.

As shown in Figure 3, malicious Hancitor documents are hosted on compromised webservers located at multiple regions globally, or they are hosted on fraud-based accounts at various hosting providers. After they establish distribution servers for a particular malspam run, the threat actors use botnet hosts to push malspam with a link to the Hancitor Word document. This malspam uses several different templates to impersonate legitimate businesses. These emails are often disguised as invoices, eFax messages, and UPS or Fedex delivery notifications, to name a few examples. If a victim clicks the embedded link, a Hancitor document is sent to the victim's computer. Figure 4 shows an example of the malspam with an embedded URL to download Hancitor in February 2017. This particular sample was a faked Amazon shipping notification. Obviously, this did not originate from Amazon: the attackers are using Amazon shipping as the plausible decoy.



Amazon.com
Your Amazon.com order has shipped (#801-35107060-4615474822)
To: [redacted]
Reply-To: Amazon.com

Yesterday at 10:46 AM

Shipping Confirmation

Hello,

Your order "Dell PowerEdge T430 5U Tower Server - 1 x Intel Xeon E5-2620 v4 Octa-core (8 Core) 2.10 GHz - 8 GB Installed DDR4 SDRAM" has shipped.
Below you can find the invoice and the shipping details.

Details

Order #801-35107060-4615474822

Expected delivery date:
February 22, 2017

Total including shipping:
$1628.99

The 'Order details' section contains an embedded URL with the download link to the hancitor sample from the distribution server.

Depending on the ship speed you chose, it may take 24 hours for tracking information to be available in your account.
We hope to see you again soon.
Amazon.com Unless otherwise noted, items sold by Amazon.com LLC are subject to sales tax in select states in accordance with the applicable laws of that state. If your order contains one or more items from a seller other than Amazon.com LLC, it may be subject to state and local sales tax, depending upon the sellers business policies and the location of their operations. Learn more about tax and seller information on our website.
This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

Figure 4: Hancitor malspam example from February 2017.

Traditionally, the link from these emails include the victim's email address as part of the URL, sometimes obfusctated using base64 or other encoding. This is likely an attempt by the Hancitor actors to track the victims who would have successfully downloaded the malicious Hancitor sample. Two examples seen earlier this year are:

- hxxp://[distribution server domain name]/api/getn.php?id=*[base64-encoded string representing recipient's email address]*
- hxxp://[distribution server domain name]/f.php?sik=[recipient's email address in plain text]

While investigating the distribution server domains, we found an open directory hosting two text files: ***visitor.txt*** and ***block.txt (Figure 6.)*** The ***visitor.txt*** file appears to track all downloads of Hancitor Word documents hosted on that server. The ***block.txt*** file appears to track IP addresses that should be blocked. Many IP addresses in the ***block.txt*** file resolved to Amazon AWS servers. We suspect this list maybe used to block analysis on automated systems run by security vendors and researchers, by not serving content to IP addresses known to be analyzing malware.

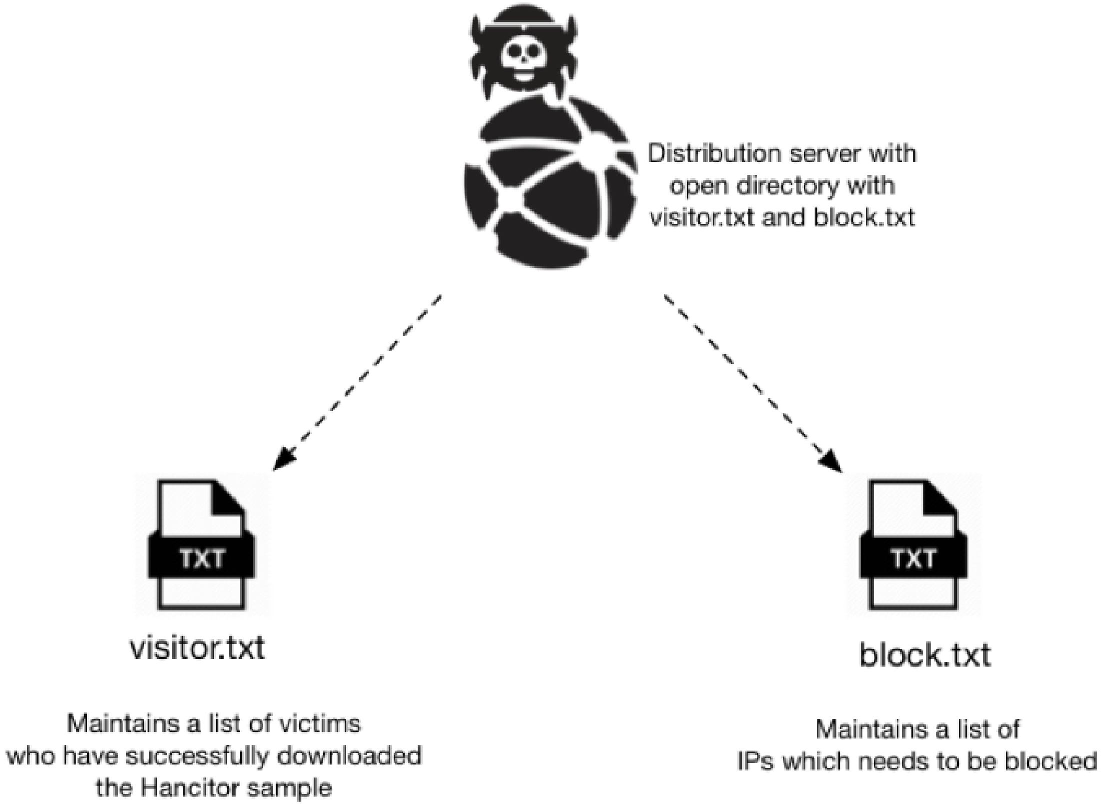
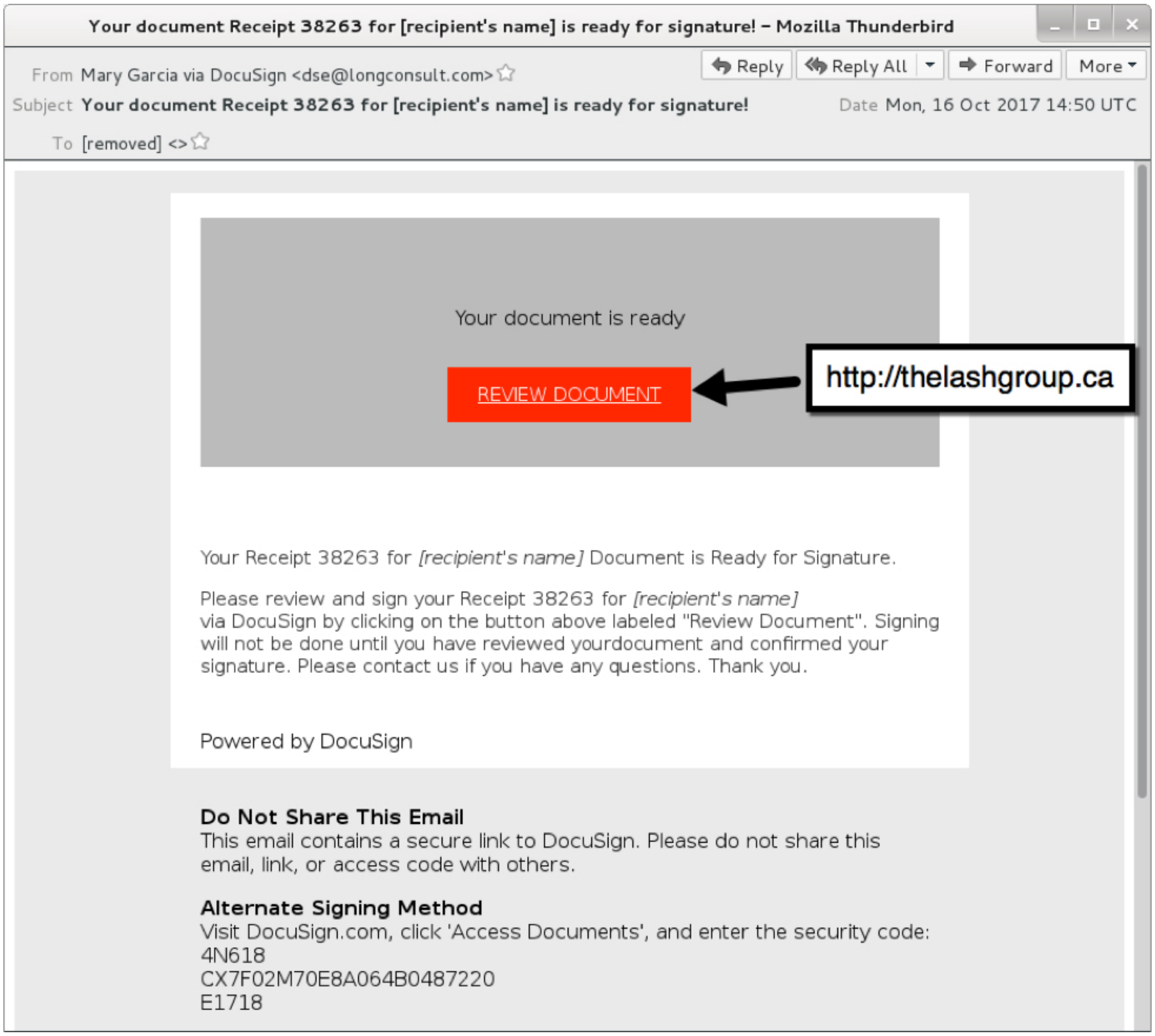

Distribution server with open directory with visitor.txt and block.txt
TXT
visitor.txt
Maintains a list of victims who have successfully downloaded the Hancitor sample
TXT
block.txt
Maintains a list of IPs which needs to be blocked

Figure 5: Text files on a distribution server hosting Hancitor documents.

Since early October 2017, these distribution servers have usually been servers set up through fraudulent accounts at hosting providers. In September through November 2017, links from Hancitor malspam occasionally resolved to these domain names without any additional text in the URL. Figure 6 shows one example.



Your document Receipt 38263 for [recipient's name] is ready for signature! – Mozilla Thunderbird

From Mary Garcia via DocuSign <dse@longconsult.com>
Subject **Your document Receipt 38263 for [recipient's name] is ready for signature!**
Date Mon, 16 Oct 2017 14:50 UTC
To [removed] <>

Your document is ready

http://thelashgroup.ca

Your Receipt 38263 for *[recipient's name]* Document is Ready for Signature.

Please review and sign your Receipt 38263 for *[recipient's name]* via DocuSign by clicking on the button above labeled "Review Document". Signing will not be done until you have reviewed yourdocument and confirmed your signature. Please contact us if you have any questions. Thank you.

Powered by DocuSign

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code:
4N618
CX7F02M70E8A064B0487220
E1718

Figure 6: Hancitor malspam example from October 2017.

In recent weeks, links from this malspam have been using a custom encoding to disguise the recipient's email address in the URL.

Distribution Server Characteristics

Given how actors behind Hancitor malspam leverage compromised servers, we investigated the numbers and regions where these servers were compromised. The below heat map provides a high-level overview of the affected countries. The distribution servers seen throughout the year are located globally. While United States accounts for a large number of distribution servers, majority of the servers in the United States are from fraudulent accounts which are hosted at hosting providers. By contrast, the majority of the distribution servers in the rest of the countries are from compromised servers belonging to legitimate businesses. According to data from January to September 2017, the majority of compromised domains used for Hancitor-based infections are located in the Asian region. Most compromised servers belong to local businesses in each country. While no specific region appears more vulnerable than others, the domains we've seen so far in 2017 imply that organizations in

Asia, especially small and medium sized businesses may be running vulnerable services likely to be exploited by the Hancitor campaign to host associated malware.

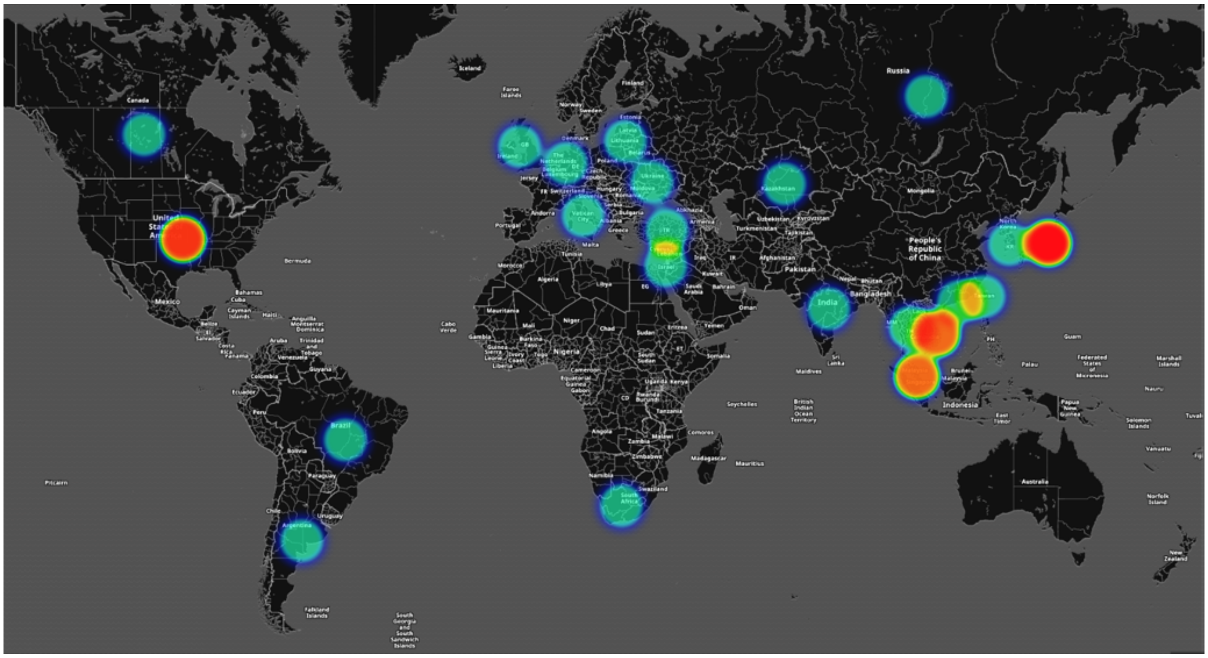


Figure 7: Hancitor distribution servers globally thus far in 2017

Country	Number of Distribution servers
United States	197
Japan	23
Vietnam	13
Singapore	12
Russia	7
Brazil	6
Malaysia	6
Hong Kong	5
South Africa	4
Thailand	4
India	2
Ireland	2
Kazakhstan	2

Taiwan	2
Turkey	2
Ukraine	2
Argentina	1
Canada	1
Germany	1
Israel	1
Italy	1
Netherlands	1
Republic of Korea	1
Republic of Lithuania	1
United Kingdom	1

Table 1 – Number of Distribution Servers by Country

As of December 2017, Hancitor Word documents have most commonly been distributed through fraudulent accounts at hosting providers. However, during post-infection activity, Hancitor downloads additional malware from additional distribution servers. These post-infection distribution servers are also legitimate websites that have been compromised by this campaign, and this characteristic of Hancitor-based infection traffic has been consistent since we started tracking Hancitor.

Common Services from Compromised Servers

Apart from web servers and other related services, almost all compromised domains were running PureFTPd or ProFTPd services. This suggests criminals behind Hancitor malspam may have been targeting servers running vulnerable versions of FTP applications. However, without any further data, we cannot make any conclusive statements.

Recent Developments

The Hancitor campaign is still evolving. Unit 42 researcher Brad Duncan recently discussed a wave of Hancitor malspam on October 16th 2017, where Word documents from the distribution servers used the DDE attack method. In this case, Hancitor was completely separated from the Word document and downloaded as a separate malware binary. This added another distribution server in the infection chain of events.The DDE attack method spread to other actors for mass-distribution of malware through email. However, by November 2017, Hancitor resumed using macros in Word documents.

Conclusion

A key factor to this campaign's longevity the abuse of hosting providers, a situation we have previously reported. Another key factor is the availability of vulnerable servers world-wide that criminals can compromise to host their malware. These are primary components in the Hancitor malspam playbook. As discussed in this blog post, we've seen an evolution in their playbook as criminals behind this campaign have fine-tuned their malware distribution techniques.Despite a somewhat limited target base of victims who disregard best security practices an run older versions of Microsoft Windows, the Hancitor campaign has remained active so far in 2017 with no extended absences. This indicates the campaign's current playbook remains cost-effective.We continue to keep a close track of this activity for further developments. Palo Alto Networks customers are protected from this threat through our next-generation security platform.

- Current samples of Hancitor are marked as Malicious by WildFire and Traps
- AutoFocus users can identify samples of this malware using the Hancitor