Cryptocurrency businesses still being targeted by Lazarus

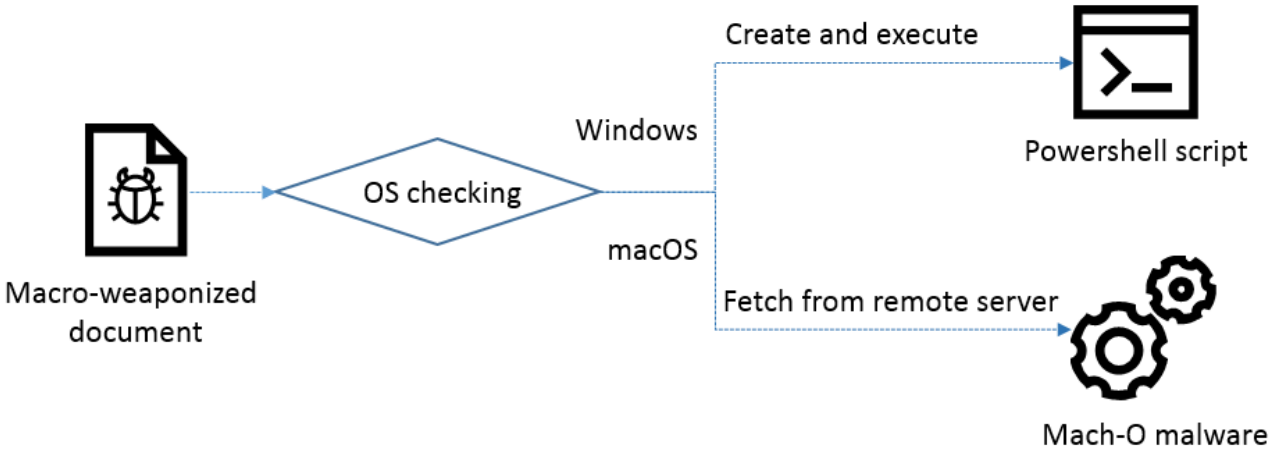
By GReAT

Published: 2019-03-26 · Archived: 2026-04-05 14:58:56 UTC

It's hardly news to anyone who follows cyberthreat intelligence that the Lazarus APT group targets financial entities, especially cryptocurrency exchanges. Financial gain remains one of the main goals for Lazarus, with its tactics, techniques, and procedures constantly evolving to avoid detection.

In the middle of 2018, we published our Operation Applejeus research, which highlighted Lazarus's focus on cryptocurrency exchanges utilizing a fake company with a backdoored product aimed at cryptocurrency businesses. One of the key findings was the group's new ability to target macOS. Since then Lazarus has been busy expanding its operations for the platform.

Further tracking of their activities targeting the financial sector enabled us to discover a new operation, active since at least November 2018, which utilizes PowerShell to control Windows systems and macOS malware for Apple users.



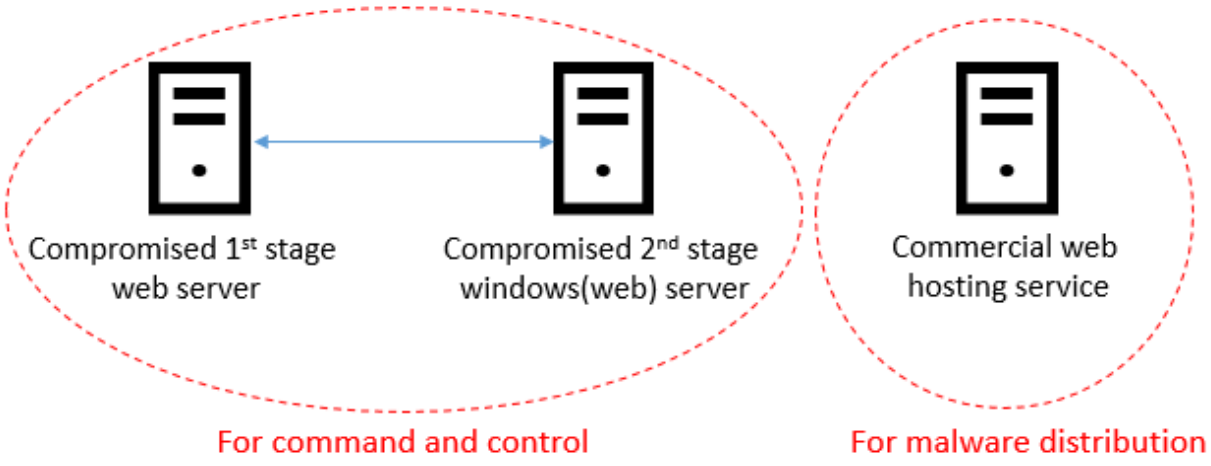
Infection procedure

Lazarus is a well-organized group, something that can be seen from their malware population: not only have we seen them build redundancy to reserve some malware in case of in-operation hot spare replacement of 'burnt' (detected) samples but they also conform to specific internal standards and protocols when developing backdoors. This case is no different. They have developed custom PowerShell scripts that communicate with malicious C2 servers and execute commands from the operator. The C2 server script names are disguised as WordPress (popular blog engine) files as well as those of other popular open source projects. After establishing the malware control session with the server, the functionality provided by the malware includes:

- Set sleep time (delay between C2 interactions)
- Exit malware

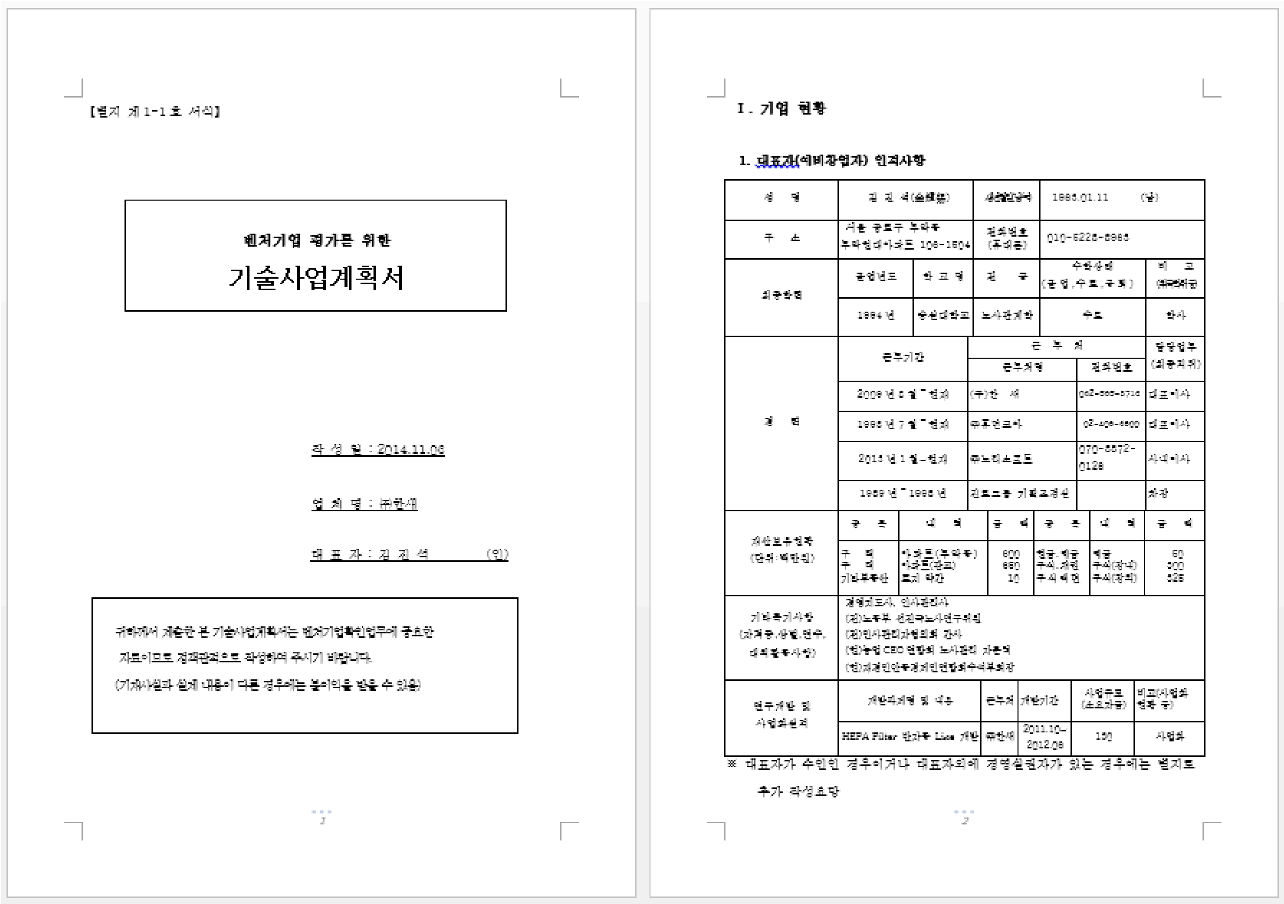
- Collect basic host information
- Check malware status
- Show current malware configuration
- Update malware configuration
- Execute system shell command
- Download & Upload files

Lazarus uses different tactics to run its C2 servers: from purchasing servers to using hacked ones. We have seen some legitimate-looking servers that are most likely compromised and used in malicious campaigns. According to server response headers, they are most likely running an old vulnerable instance of Internet Information Services (IIS) 6.0 on Microsoft Windows Server 2003. Another C2 server was probably purchased by Lazarus from a hosting company and used to host macOS and Windows payloads. The geography of the servers varies, from China to the European Union. But why use two different types of servers? The group seems to have a rule (at least in this campaign) to only host malware on rented servers, while hosting C2 scripts for malware communication on compromised servers.



Infrastructure segregation by purpose

The malware was distributed via documents carefully prepared to attract the attention of cryptocurrency professionals. Seeing as how some of the documents were prepared in Korean, we believe that South Korean businesses are a high priority for Lazarus. One document entitled ‘Sample document for business plan evaluation of venture company’ (translated from Korean) looks like this:


[별지 제 1-1 호 서식]

벤처기업 평가를 위한

기술사업계획서

작 성 일 : 2014.11.06

업 체 명 : (주)한새

대 표 자 : 김 진 석 (인)

귀하께서 제출한 본 기술사업계획서는 벤처기업확인업무에 중요한 자료이므로 정확한 객관적으로 작성하여 주시기 바랍니다.

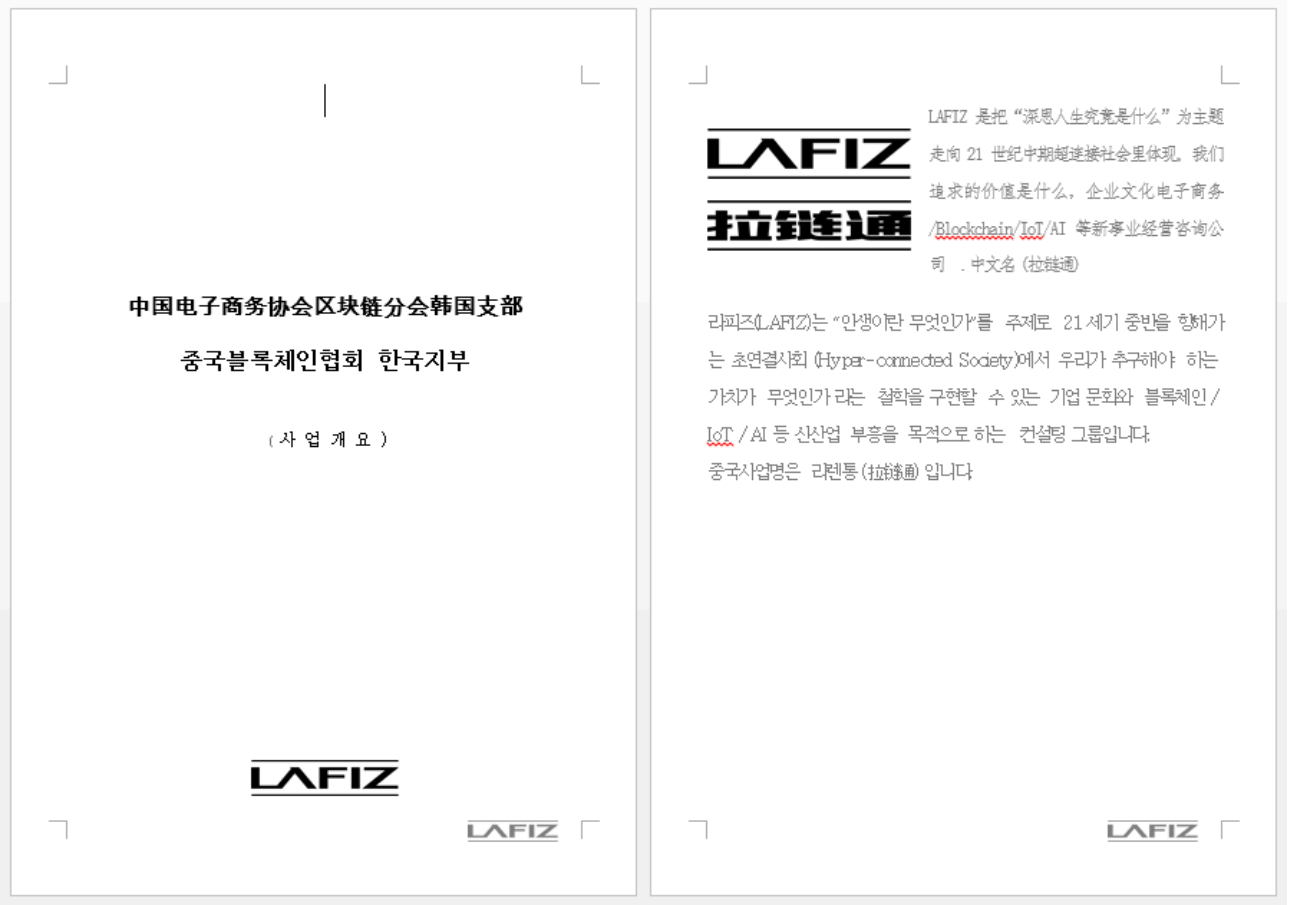
(기재사실과 실제 내용이 다른 경우에는 불이익을 받을 수 있음)

I. 기업 현황

1. 대표자(예비창업자) 인적사항

Content of weaponized document from Lazarus (4cbd45fe6d65f513447beb4509a9ae3d)

Another macro-weaponized document (e9a6a945803722be1556fd120ee81199) contains a business overview of what seems to be a Chinese technology consulting group named LAFIZ. We couldn't confirm if it's a legitimate business or another fake company made up by Lazarus. Their website lafiz[.]link has been parked since 2017.



中国电子商务协会区块链分会韩国支部

중국블록체인협회 한국지부

（사 업 개 요）

LAFIZ

LAFIZ

LAFIZ 是把“深思人生究竟是什么”为主题走向 21 世纪中期超连接社会里体现。我们追求的价值是什么，企业文化电子商务/Blockchain/IoT/AI 等新事业经营咨询公司 . 中文名 (拉链通)

라피즈(LAFIZ)는 "인생이란 무엇인가"를 주제로 21세기 중반을 향해가는 초연결사회 (Hyper-connected Society)에서 우리가 추구해야 하는 가치가 무엇인가라는 철학을 구현할 수 있는 기업 문화와 블록체인/IoT/AI 등 신산업 부흥을 목적으로 하는 컨설팅 그룹입니다.
중국사업명은 라롄통(拉链通) 입니다.

LAFIZ

Contents of another weaponized document (e9a6a945803722be1556fd120ee81199)

Based on our telemetry, we found a cryptocurrency exchange company attacked with a malicious document containing the same macro. The document's content provided information for coin listings with a translation in Korean:

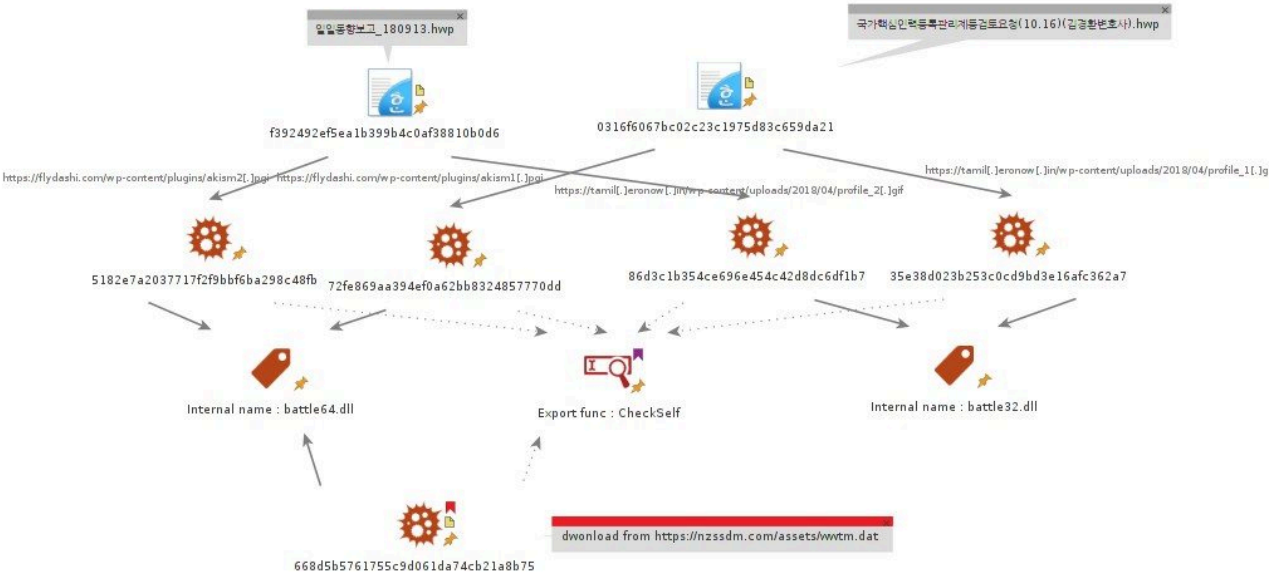
Coin Information (코인정보)

Item			Information	Example
General	Coin Name	영문 코인명		
	Coin Name in Korean	한글 코인명		
	Ticker	심볼코드		
	Foundation	재단(법인)명		
	Location	재단(법인) 소재지		
	Founded Date	재단 설립일		
	Founder / CEO	설립자		경력을 기술해야 하나요?
	Developer / CTO	핵심 개발자		경력을 기술해야 하나요?
	Advisor	주요 자문위원		자문위원들에 대한 구체적인 소개가 필요한지...?
	Partner	주요 협력사		협력사가 많은데 다 열거해야 하는지..?
URL	Homepage	홈페이지		
	Blockchain Explorer	블록체인 탐색 주소		
	White Paper	백서 주소		
	Link at Etherscan.io	이더스캔 주소		
	Wallet Download	개인지갑 다운로드		
	Source Code (Git)	소스코드 주소		
Supply	Issued date	최초 발행일		
	Max Supply	최대 공급량		
	Circulating Supply	유통 공급량		
	Amount of Pre-mining	사전 채굴량		

Content of another weaponized document (6a0f3abd05bc75edbfb862739865a4cc)

The payloads show that Lazarus keeps exploring more ways to evade detection to stay under the radar longer. The group builds malware for 32-bit and 64-bit Windows separately to support both platforms and have more variety in terms of compiled code. The Windows payloads distributed from the server (nzssdm[.]com) hosting the Mac malware have a CheckSelf export function, and one of them (668d5b5761755c9d061da74cb21a8b75) has the internal name 'battle64.dll'. From that point we managed to find additional Windows malware samples containing the CheckSelf export function and an internal name containing the word 'battle'.

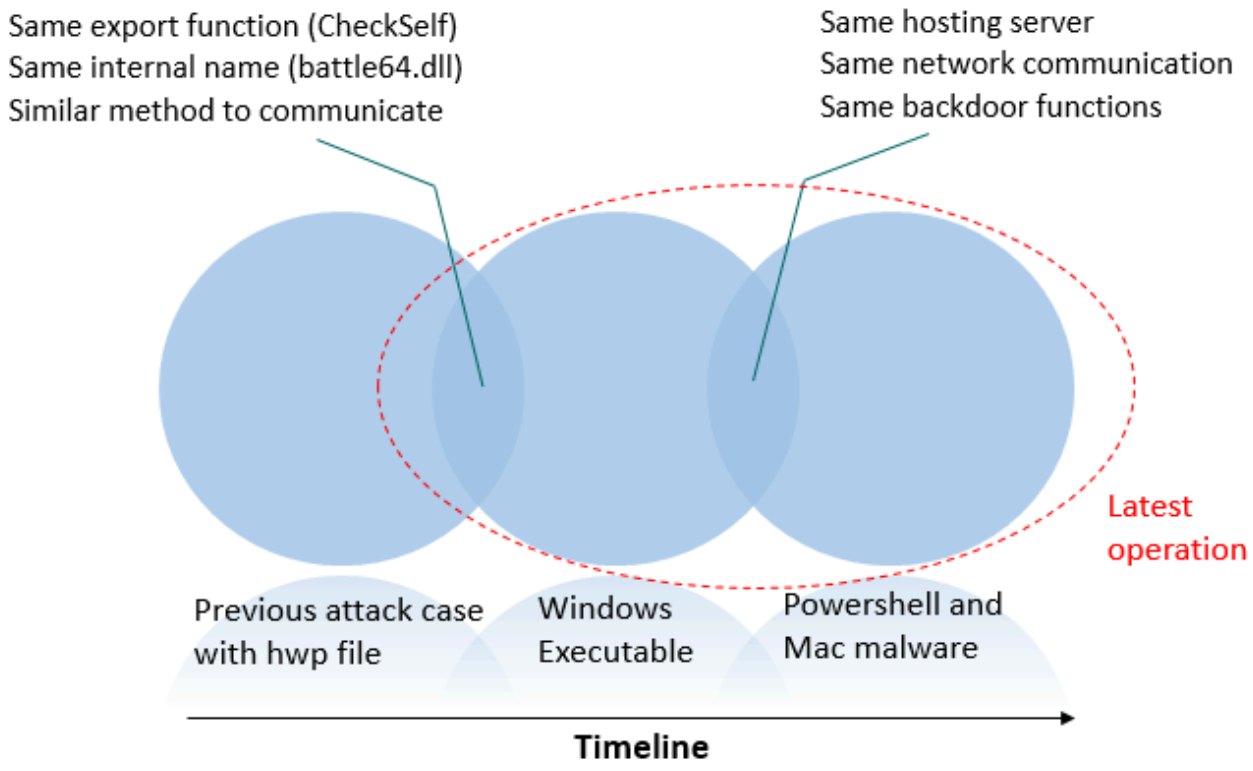
These Windows malware samples were delivered using malicious HWP (Korean Hangul Word Processor format) documents exploiting a known PostScript vulnerability. It should be noted that HWP documents are only popular among Korean users (Hangul Word Processor was developed in South Korea) and we have witnessed several attacks using the same method.



Connection with previous HWP attacks

It's no secret that Apple products are now very popular among successful internet startups and fintech companies, and this is why the malicious actor built and used macOS malware. While investigating earlier Lazarus incidents, we anticipated this actor would eventually expand its attacks to macOS.

It appears that Lazarus is using the same developers to expand to other platforms, because some of the features have remained consistent as its malware evolves.



Overlap of current campaign and previous hwp-based attack cases

We'd therefore like to ask Windows and macOS users to be more cautious and not fall victim to Lazarus. If you're part of the booming cryptocurrency or technological startup industry, exercise extra caution when dealing with new third parties or installing software on your systems. It's best to check new software with an antivirus or at least use popular free virus-scanning services such as VirusTotal. And never 'Enable Content' (macro scripting) in Microsoft Office documents received from new or untrusted sources. Avoid being infected by fake or backdoored software from Lazarus – if you need to try out new applications, it's better do so offline or on an isolated network virtual machine which you can erase with a few clicks. We'll continue posting on Lazarus's latest tactics and tricks in our blog. In the meantime, stay safe!

For more details on this and other research, please contact intelreports@kaspersky.com.

File Hashes:

Malicious office document used in real attack
4cbd45fe6d65f513447beb4509a9ae3d 샘플_기술사업계획서(벤처기업평가용).doc
6a0f3abd05bc75edbfb862739865a4cc 문의_Evaluation Table.xls

Testing office document
29a37c6d9fae5664946c6607f351a8dc list.doc
e9a6a945803722be1556fd120ee81199 list.doc
a18bc8bc82bca8245838274907e64631 list.doc

macOS malware

4345798b2a09fc782901e176bd0c69b6

PowerShell script

cb713385655e9af0a2fc10da5c0256f5 test.ps1

e6d5363091e63e35490ad2d76b72e851 test.ps1 – It does not contain URLs.

Da4981df65cc8b5263594bb71a0720a1

Windows executable payload

171b9135540f89bf727b690b9e587a4e wwtm.dat

668d5b5761755c9d061da74cb21a8b75 wwtm.dat

ad3f966d48f18b5e7b23a579a926c7e8

Manuscrypt payload

35e38d023b253c0cd9bd3e16afc362a7

72fe869aa394ef0a62bb8324857770dd

86d3c1b354ce696e454c42d8dc6df1b7

5182e7a2037717f2f9bbf6ba298c48fb

Malicious hwp file

F392492ef5ea1b399b4c0af38810b0d6 일일동향보고_180913.hwp

0316f6067bc02c23c1975d83c659da21 국가핵심인력등록관리제등검토요청(10.16)(김경환변호사).hwp

Domains and IPs

Compromised first stage C2 server

http://bluecreekrobotics[.]com/wp-includes/common.php

http://dev.microcravate[.]com/wp-includes/common.php

http://dev.whatsyourcrunch[.]com/wp-includes/common.php

http://enterpriseheroes.com[.]ng/wp-includes/common.php

http://hrgp.asselsolutions[.]com/wp-includes/common.php

https://baseballcharlemagnelegardeur[.]com/wp-content/languages/common.php

https://bogorcenter[.]com/wp-content/themes/index2.php

https://eventum.cwsdev3.bi[.]com/wp-includes/common.php

https://streamf[.]ru/wp-content/index2.php

https://towingoperations[.]com/chat/chat.php

https://vinhsake[.]com//wp-content/uploads/index2.php

https://www.tangowithcolette[.]com/pages/common.php

Second stage C2 server

http://115.28.160[.]20:443 – Compromised server

Malware hosting server

http://nzssdm[.]com/assets/wwtm.dat – Windows payload distribution URL

http://nzssdm[.]com/assets/mt.dat – Mac payload distribution URL
