ECHO

CYBER THREAT INTELLIGENCE

LAZARUS (APT-38) Analysis REPORT

Content

Executive Summery

This report aims to provide a detailed analysis of the Lazarus APT group, evaluating their activities, targets, and the attack techniques they have employed. The Lazarus APT group is a long-standing and internationally active threat actor known for engaging in various sectors with complex attack campaigns for financial gain, espionage, and cyber sabotage.

The report delves into the technical capabilities and attack strategies of the Lazarus APT group by examining prominent past attack campaigns and their targets. The sectors they have targeted include finance, energy, media, technology, and the public sector. Furthermore, the report explores how the group utilizes techniques such as social engineering, malware injection, and advanced persistent threats to reach their objectives.

In addition to their advanced attack capabilities, the report highlights the group's skills in target identification and concealing long-term espionage activities. The Lazarus APT group continuously evolves their cyber attacks, persistently challenging security experts and defense mechanisms.

In conclusion, this report underscores the significance of the Lazarus APT group in the realm of cyber threats, emphasizing the need for organizations to bolster their defense strategies and develop more effective protection methods against advanced attacks. Understanding the group's activities and implementing countermeasures are critical necessities for the cybersecurity community.

Introduction

As cybersecurity threats become increasingly sophisticated and complex, hackers and cyber adversaries are employing evolving techniques to carry out attacks on an unprecedented scale. In this context, long-standing and versatile threat actors like the Lazarus APT group have captured the attention of cybersecurity experts and defense mechanisms. The Lazarus APT group has conducted intricate attacks targeting a wide range of sectors on an international level, with goals encompassing financial gain, espionage, and cyber sabotage.

This report aims to provide an in-depth examination of the activities of the Lazarus APT group, offering a comprehensive overview of their attack techniques, targets, and operations. By evaluating prominent past attack campaigns and their respective targets, the report seeks to enhance our understanding of the group's methods and strategies.

The activities of the Lazarus APT group hold significance for cybersecurity experts and industry leaders. Their targeted sectors span finance, energy, media, technology, and the public sector. The objective of this report is to assist cybersecurity professionals and decision-makers in adopting more effective defense measures against potential threats posed by the Lazarus APT group by studying their attack capabilities, strategies, and operations.

Subsequently, the report will delve into the group's notable attack campaigns, types of malware employed, attack vectors, and tactics used to target specific entities. Furthermore, the report will assess the group's advanced capabilities in the realm of cybersecurity and their international scope of operations.

Countries and Sectors Targeted by the Lazarus APT Group

The Lazarus APT group has established a broad range of targets on an international scale through its long-standing activities. The group has carried out complex attacks with the intent of financial gain, espionage, and cyber sabotage, targeting specific countries and sectors.

1. Financial Sector:

The Lazarus APT group has carried out attacks targeting numerous organizations within the financial sector. Banks, financial institutions, and cryptocurrency exchanges have been significant targets for the group. In pursuit of financial gains, the group has launched attacks against its targets through malicious software, causing substantial losses.

2. Energy and Defense Sector:

The energy and defense sectors have been focal points of Lazarus APT group's cyber espionage activities. The group has employed advanced attack techniques to access sensitive information related to energy companies and the defense industry. The targets within these sectors can pose a significant threat to national security, given the group's use of sophisticated attack methods to gain access to critical information.

3. The Technology and Telecommunications Sector:

The Lazarus APT group has carried out attacks targeting companies operating in the technology and telecommunications sectors. The targets within these sectors can be subjected to attacks aiming to steal trade secrets, gain access to innovative technologies, and acquire strategic information.

4. Public and Political Organizations:

Lazarus APT group has also conducted attacks against the public sector and political organizations. Such targets may involve espionage activities for political reasons or aiming to impact national security. The group has launched large-scale cyber attacks by targeting government agencies and international organizations.

5. Media and Entertainment Sector:

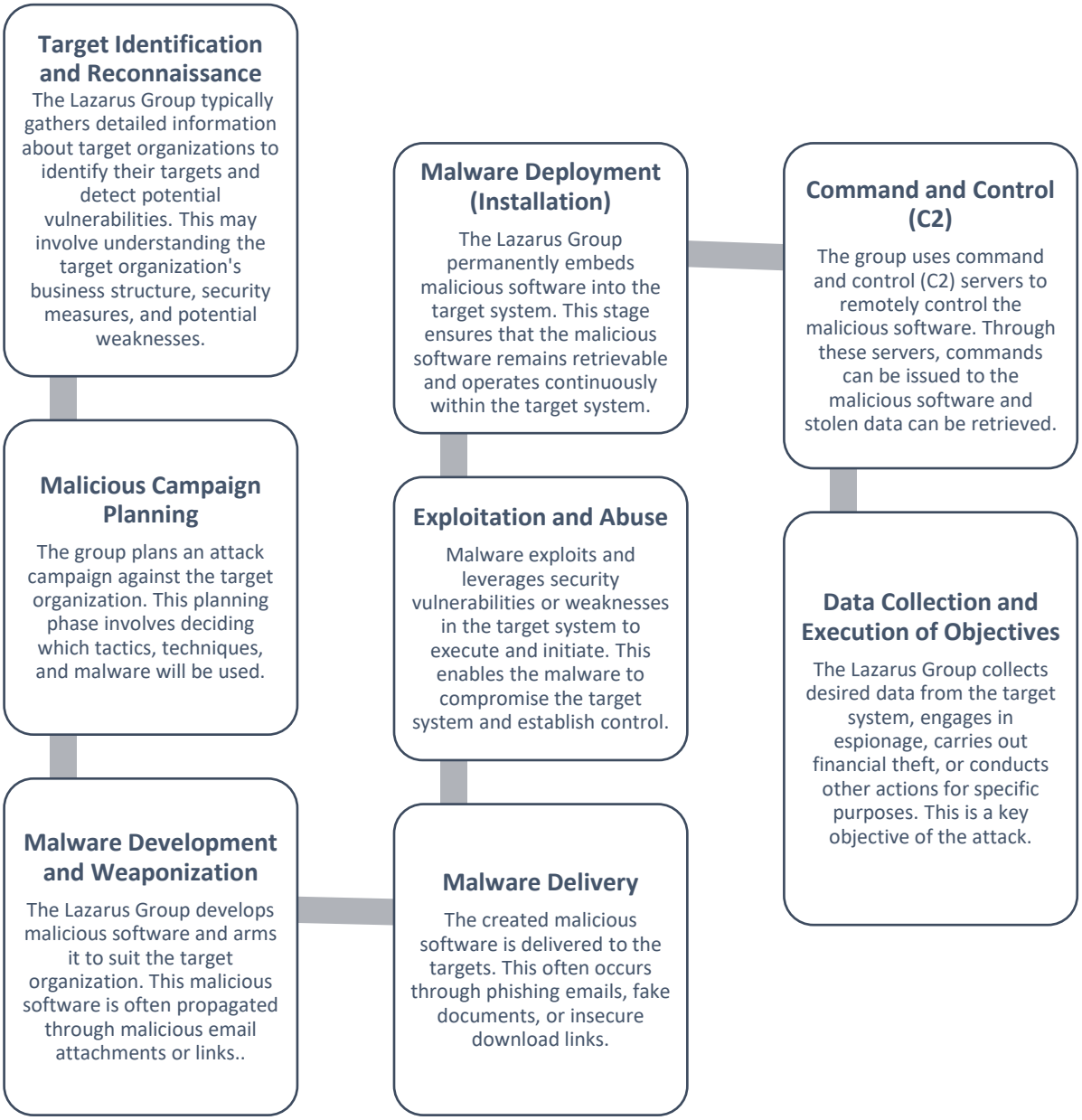
Medya ve eğlence sektörü de Lazarus APT grubunun hedeflerinden biridir. Bu sektördeki hedefler, ünlü kişilerin verilerinin çalınması, sansürü aşma veya propaganda amaçlarına yönelik olabilir.

The diversity of countries and sectors targeted by the Lazarus APT group demonstrates the breadth of their operations and strategies. The ability to target numerous sectors and countries of this kind positions the group as a significant threat to international cybersecurity.

Information is available regarding the countries among which the Lazarus APT group has targeted. The following countries are included:

- Taiwan
- China
- Germany
- India
- Russia
- Brazil
- Singapore
- Indonesia
- Vietnam
- South Korea
- Japan
- United States
- United Kingdom
- Australia
- Turkey
- Saudi Arabia

Attack Chain



Attack and Campaigns

Attacks

Crypto payment service provider CoinsPaid fell victim to a cyberattack resulting in the theft of $37.2 million worth of cryptocurrency.

Lazarus targets vulnerable Microsoft IIS servers to distribute malicious software.

The Lazarus APT group exploited a zero-day vulnerability in attacks targeting a South Korean financial entity.

The FBI confirmed that the Lazarus APT group was behind the $100 million cyber heist on Harmony Horizon Bridge.

Lazarus was associated with a cyber attack targeting the IT infrastructure and email server of NPO Mashinostroyeniya, a Russian space rocket designer and intercontinental ballistic missile engineering organization.

Blockchain analysts attribute the recent attack on the payment processing platform Alphapo, resulting in the theft of around 60 million dollars' worth of cryptocurrency, to the North Korean Lazarus group.

Campaigns

Operation Dream Job (C0022)

Operation Dream Job is a comprehensive and sophisticated cyber espionage campaign initiated by the Lazarus APT group in 2019. The Lazarus APT group is recognized for its long-standing activities and is a globally-reaching cyber threat actor group.

Campaign Initiation and Objectives:

The Operation Dream Job campaign is a complex espionage endeavor initiated by the Lazarus APT group for financial purposes. The campaign targets organizations in the financial sector with the aim of achieving financial gain. Among the targets are banks, financial institutions, cryptocurrency exchanges, and other finance-related sectors. The primary objectives of the campaign include:

- Gaining access to the content of financial institutions and stealing account information.
- Infiltrating cryptocurrency exchanges to seize digital assets.
- Injecting malicious software into banking systems to manipulate financial transactions.
- Campaign's Technical Structure and Methods:

The Operation Dream Job campaign employs advanced cyber attack techniques. These techniques include social engineering, phishing attacks, malware injection, and sophisticated persistent threats. The campaign attacks its targets using the following methods:

Spear Phishing: Delivering malware to targeted organizations through customized phishing emails.

Malicious Attachments: Encouraging victims to open malicious attachments by using enticing subjects like fake job applications.

Backdoor Creation: Developing backdoors to enable the infiltration of malicious software into target systems.

Command and Control (C2) Servers: Establishing C2 servers to communicate with compromised systems and issue commands."

AppleJeus (S0584)

AppleJeus is a downloader family that was initially discovered in 2018 embedded in trojanized cryptocurrency applications. It is attributed to the Lazarus Group. AppleJeus has been used to target companies in the energy, finance, government, industrial, technology, and telecommunications sectors, as well as several countries including the United States, United Kingdom, South Korea, Australia, Brazil, New Zealand, and Russia. AppleJeus has been utilized to distribute the FALLCHILL RAT.

DTrack BackDoor (S0567)

Dtrack is a spyware that was discovered in 2019 and was used against Indian financial institutions, research facilities, and the Kudankulam Nuclear Power Plant. It shares similarities with the DarkSeoul campaign attributed to the Lazarus Group.

Dtrack allows attackers to collect information from the infected host computer, upload/download/manipulate files to/from the infected host, exfiltrate data, and execute commands.

WannaCry (S0366)

WannaCry is a type of ransomware that triggered a major global cybersecurity attack in 2017, impacting millions of computers worldwide.

Emergence and Spread of WannaCry Ransomware

WannaCry ransomware emerged suddenly in May 2017 and quickly triggered a global crisis. This attack is an example of the ransomware type, where malicious actors lock computer systems and demand ransom from victims. WannaCry exploited a security vulnerability (MS17-010) in Windows operating systems to spread, affecting numerous computers.

After encrypting computer files, the attack made it impossible to recover data without paying the ransom. WannaCry coerced users with the threat that files would be permanently lost if the ransom was not paid, inducing panic and distress.

Global Impacts and Significance

The WannaCry ransomware attack impacted numerous organizations, hospitals, government agencies, and individual users on a global scale. This event highlighted the critical nature of cybersecurity. It also emphasized that cyberattacks can pose threats not only to financial well-being but also to people's health and safety. The WannaCry attack served as an example of how cybersecurity risks can affect not only companies but also public services and citizens.

Most Commonly Used Malware Families by Lazarus Group

EarlyRAT

An offshoot of the Lazarus APT group, a subgroup known as Andariel, has been discovered using an undisclosed remote access Trojan (RAT) named 'EarlyRAT'.

EarlyRAT was uncovered around mid-2022, during which threat actors leveraged Log4Shell to breach corporate networks.

EarlyRAT bears resemblance to another tool used by Lazarus, MagicRAT, which involves creating scheduled tasks and downloading additional malicious payloads from the command and control (C2) server.

MagicRat

MagicRat is a malicious software family used to infiltrate target systems and facilitate data theft. It is commonly spread through social engineering tactics and malicious emails, distracting users and enabling unauthorized access to systems. MagicRat is employed to conduct covert espionage activities and steal sensitive information.

TigerRAT

TigerRAT is a sophisticated cyber espionage tool that primarily targets Asian-based objectives. This toolkit infiltrates target systems through phishing emails or malicious links, aiming to steal data, conduct espionage, or establish remote control. TigerRAT is employed to gather advanced threat intelligence and monitor the activities of targets.

TrickBot

TrickBot is known as a Trojan specifically designed for targeting the financial sector. It aims to steal users' bank account information, credit card data, and other financial details. Additionally, it may also include ransomware features and demand ransom through data encryption. TrickBot is a threat commonly used by Lazarus for financial gain.

Lazarus Group's Exploited Vulnerabilities

- **Log4j**
- **CVE-2018-4878**
- **CVE-2021-31166**
- **CVE-2021-31176**
- **CVE-2021-31178**
- **CVE-2021-31207**
- **CVE-2008-5007**
- **CVE-2006-3616**
- **CVE-2007-1486**
- **CVE-2014-4610**
- **CVE-2014-4609**
- **CVE-2014-4608**
- **CVE-2014-4611**
- **CVE-2014-4607**
- **CVE-2014-4610**
- **CVE-2014-4608**

YARA RULE

```
import "hash"

rule Rule_MagicRAT

{

meta:

        author="Bilal BAKARTEPE & Bugra KOSE"

        description="MagicRAT Analysis"

strings:

        $opc1="53 48 83 EC 20 B8 01 00 00 00 48 89 CB 48 85 C9 48 0F 44 D8 48 89 d9
E8 7C 73 3A FF 48 85 C0 74 0F 48 83 C4 20 5B C3"


condition:

        hash.md5(0,filesize) == "aea6585be1b8ed83061e13b72e2f21d7" or $opc1


}
```

SIGMA RULES

SIGMA RULE 1

```
title: MagicRAT Malware Family
status: experimental
description: Detects MagicRAT Network Behaviours.
author: Bilal BAKARTEPE & Buğra KÖSE
date: 2023/08/10
tags:
    - attack.persistence
    - attack.T1082
    - attack.T1071.001
    - attack.T1059.003
logsource:
    category: network_connection
    product: windows
detection:
    selection:
        cs-method: 'GET'
        resource.URL:
        - 64.188.27.73.static.quadranet.com
        - 172.16.3.81
        - p409198-omed01.tokyo.ocn.ne.jp
        - gendoraduragonkgp126.com/
    condition: selection
fields:
    - RAT
    - Lazarus
level: critical
```

SIGMA RULE 2

```
title: MagicRAT Malware Family
status: experimental
description: Detects MagicRAT Process Behaviours.
author: Bilal BAKARTEPE & Buğra KÖSE
date: 2023/08/10
tags:
    - attack.persistence
    - attack.T1082
    - attack.T1071.001
    - attack.T1059.003
logsource:
    category: process_creation
    product: windows
detection:
    selection1:
        TargetImage: cmd.exe
    selection2:
        CommandLine:
        - cmd.exe  /c bcdedit
    selection3:
        TargetImage: schtasks.exe
    selection4:
        CommandLine:
        - '/create /tn \"OneDrive AutoRemove\" /tr \"C:\Windows\System32\cmd.exe /c del /f /q C:/Users/user/Desktop/'
        - '/sc daily /st 10:30:30 /ru SYSTEM'
    selection5:
        CommandLine:
        - 'schtasks /create /tn \"OneDrive AutoRemove\" /tr \"C:\Windows\System32\cmd.exe /c del /f /q
C:/Users/user/Desktop/'
        - '/sc daily /st 10:30:30 /ru SYSTEM'
    selectionHash:
        event_id: 1
        event_data.Hashes:
        - 586F30907C3849C363145BFDCDABE3E2E4688CBD5688FF968E984B201B474730
        - 8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5
        - c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f
        - dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469
        - 90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4
        - 226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb
        - 16F413862EFDA3ABA631D8A7AE2BFFF6D84ACD9F454A7ADAA518C7A8A6F375A5
        - 05732E84DE58A3CC142535431B3AA04EFBE034CC96E837F93C360A6387D8FAAD
        - 6FBB771CD168B5D076525805D010AE0CD73B39AB1F4E6693148FE18B8F73090B
        - 912018AB3C6B16B39EE84F17745FF0C80A33CEE241013EC35D0281E40C0658D9
        - CAF6739D50366E18C855E2206A86F64DA90EC1CDF3E309AEB18AC22C6E28DC65
        - 2963a90eb9e499258a67d8231a3124021b42e6c70dacd3aab36746e51e3ce37e
        - 2AA1BBBE47F04627A8EA4E8718AD21F0D50ADF6A32BA4E6133EE46CE2CD13780
        - 5A73FDD0C4D0DEEA80FA13121503B477597761D82CF2CFB0E9D8DF469357E3F8
        - C92C158D7C37FEA795114FA6491FE5F145AD2F8C08776B18AE79DB811E8E36A3
    condition: (selection1 and selection2) or (selection1 and selection5) or (selection3 and selection4) or (selectionHash)
fields:
    - RAT
    - Lazarus
level: critical
```

IoC's

Hashs

586F30907C3849C363145BFDCDABE3E2E4688CBD5688FF968E984B201B474730	VSingle
8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5	MagicRAT
c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f	MagicRAT
dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469	MagicRAT
90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4	MagicRAT
226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb	YamaBotf
16F413862EFDA3ABA631D8A7AE2BFFF6D84ACD9F454A7ADAA518C7A8A6F375A5	Procdump
05732E84DE58A3CC142535431B3AA04EFBE034CC96E837F93C360A6387D8FAAD	Procdump
6FBB771CD168B5D076525805D010AE0CD73B39AB1F4E6693148FE18B8F73090B	Mimikatz
912018AB3C6B16B39EE84F17745FF0C80A33CEE241013EC35D0281E40C0658D9	Mimikatz
CAF6739D50366E18C855E2206A86F64DA90EC1CDF3E309AEB18AC22C6E28DC65	Mimikatz
2963a90eb9e499258a67d8231a3124021b42e6c70dacd3aab36746e51e3ce37e	3Proxy
2AA1BBBE47F04627A8EA4E8718AD21F0D50ADF6A32BA4E6133EE46CE2CD13780	PuTTY
5A73FDD0C4D0DEEA80FA13121503B477597761D82CF2CFB0E9D8DF469357E3F8	PuTTY
C92C158D7C37FEA795114FA6491FE5F145AD2F8C08776B18AE79DB811E8E36A3	Adfind

IPs

1[.]251[.]44[.]118	51[.]68[.]119[.]230
101[.]0[.]115[.]80	51[.]79[.]44[.]111
103[.]227[.]176[.]20	54[.]241[.]91[.]49
110[.]10[.]189[.]166	54[.]39[.]64[.]114
110[.]45[.]138[.]98	104[.]155[.]149[.]103
112[.]175[.]226[.]221	40[.]121[.]90[.]194
114[.]207[.]112[.]202	185[.]29[.]8[.]162
115[.]23[.]252[.]233	146[.]4[.]21[.]94
118[.]217[.]183[.]180	46[.]183[.]221[.]109
210[.]217[.]137[.]70	84[.]38[.]133[.]145
211[.]115[.]65[.]71	109[.]248[.]150[.]13
211[.]202[.]2[.]195	155[.]94[.]210[.]11
212[.]227[.]91[.]36	192[.]186[.]183[.]133
217[.]69[.]41[.]33	54[.]68[.]42[.]4
31[.]186[.]8[.]221	213[.]180[.]180[.]154
50[.]192[.]28[.]29	172[.]16[.]3[.]81

URLs

hxxp[://]104[.]155[.]149[.]103/2-443[.]ps1
hxxp[://]104[.]155[.]149[.]103/8080[.]ps1
hxxp[://]104[.]155[.]149[.]103/mi64[.]tmp
hxxp[://]104[.]155[.]149[.]103/mi[.]tmp
hxxp[://]104[.]155[.]149[.]103/mm[.]rar
hxxp[://]104[.]155[.]149[.]103/pd64[.]tmp
hxxp[://]104[.]155[.]149[.]103/rar[.]tmp
hxxp[://]104[.]155[.]149[.]103/spr[.]tmp
hxxp[://]104[.]155[.]149[.]103/t[.]tmp
hxxp[://]104[.]155[.]149[.]103/update[.]tmp
hxxp[://]109[.]248[.]150[.]13:8080/1
hxxp[://]146[.]4[.]21[.]94/tmp/data_preview/virtual[.]php
hxxp[://]185[.]29[.]8[.]162:443/1[.]tmp
hxxp[://]40[.]121[.]90[.]194/11[.]jpg
hxxp[://]40[.]121[.]90[.]194/300dr[.]cert
hxxp[://]40[.]121[.]90[.]194/b[.]cert
hxxp[://]40[.]121[.]90[.]194/qq[.]cert
hxxp[://]40[.]121[.]90[.]194/ra[.]cert
hxxp[://]40[.]121[.]90[.]194/Rar[.]jpg
hxxp[://]40[.]121[.]90[.]194/tt[.]rar
hxxp[://]46[.]183[.]221[.]109//dfdfdfdfdfdfdfdfdfaflakjdfljaldjfladfljaldkfjlajdsflajdskf/hunterroy[.]exe
hxxp[://]46[.]183[.]221[.]109//dfdfdfdfdfdfdfdfdfaflakjdfljaldjfladfljaldkfjlajdsflajdskf/svhostw[.]exe
hxxp[://]84[.]38[.]133[.]145/board[.]html
hxxp[://]84[.]38[.]133[.]145/header[.]xml
hxxp[://]www[.]ajoa[.]org/home/manager/template/calendar[.]php
hxxp[://]www[.]ajoa[.]org/home/rar[.]tmp
hxxp[://]www[.]ajoa[.]org/home/tmp[.]ps1
hxxp[://]www[.]ajoa[.]org/home/ztt[.]tmp
hxxp[://]www[.]orvi00[.]com/ez/admin/shop/powerline[.]tmp
hxxp[://]64[.]188[.]27[.]73[.]static[.]quadranet[.]com
hxx[://]p409198-omed01[.]tokyo[.]ocn[.]ne[.]jp
https[:]//angeldonationblog[.]com/image/upload/upload.php
https[:]//codevexillium[.]org/image/download/download.asp
https[:]//investbooking[.]de/upload/upload.asp

https[:]//transplugin[.]io/upload/upload.asp
https[:][//www.dronerc](https://www.dronerc/)[.]it/forum/uploads/index.php
https[:][//www.dronerc](https://www.dronerc/)[.]it/shop_testbr/Core/upload.php
https[:][//www.dronerc](https://www.dronerc/)[.]it/shop_testbr/upload/upload.php
https[:][//www.edujikim](https://www.edujikim/)[.]com/intro/blue/insert.asp
https[:][//www.fabioluciani](https://www.fabioluciani/)[.]com/es/include/include.asp
http[:]//trophylab[.]com/notice/images/renewal/upload.asp
http[:][//www.colasprint](https://www.colasprint/)[.]com/_vti_log/upload.asp

Domains

markettrendingcenter[.]com
lm-career[.]com
advantims[.]com
angeldonationblog[.]com
codevexillium[.]org
investbooking[.]de
krakenfolio[.]com
opsonew3org[.]sg
transferwiser[.]io
transplugin[.]io

VSingle C2s

hxxps[://]tecnojournals[.]com/review
hxxps[://]semiconductboard[.]com/xml
hxxp[://]cyancow[.]com/find

MagicRAT C2s

hxxp[://]155[.]94[.]210[.]11/news/page[.]php
hxxp[://]192[.]186[.]183[.]133/bbs/board[.]php
hxxp[://]213[.]32[.]46[.]0/board[.]php
hxxp[://]54[.]68[.]42[.]4/mainboard[.]php
hxxp[://]84[.]38[.]133[.]145/apollom/jeus[.]php
hxxp[://]mudeungsan[.]or[.]kr/gbbs/bbs/template/g_botton[.]php
hxxp[://]www[.]easyview[.]kr/board/Kheader[.]php
hxxp[://]www[.]easyview[.]kr/board/mb_admin[.]php

YamaBot C2s

hxxp[://]213[.]180[.]180[.]154/editor/session/aaa000/support[.]php

Other C2s

http://www.ikrea.or[.]kr/main/main_board.asp
http://www.fored.or[.]kr/home/board/view.php
https://www.zndance[.]com/shop/post.asp
http://www.cowp.or[.]kr/html/board/main.asp
http://www.style1.co[.]kr/main/view.asp
http://www.erpmas.co[.]kr/Member/franchise_modify.asp
https://www.wowpress.co[.]kr/customer/refuse_05.asp
https://www.quecue[.]kr/okproj/ex_join.asp
http://www.pcdesk.co[.]kr/Freeboard/mn_board.asp
http://www.gongsinet[.]kr/comm/comm_gongsi.asp
http://www.goojoo[.]net/board/banner01.asp
http://www.pgak[.]net/service/engine/release.asp
https://www.gncaf.or[.]kr/cafe/cafe_board.asp
https://www.hsbutton.co[.]kr/bbs/bbs_write.asp
https://www.hstudymall.co[.]kr/easypay/web/bottom.asp

SHA-1

3D311117D09F4A6AD300E471C2FB2B3C63344B1D	SHA-1
3ABFEC6FC3445759730789D4322B0BE73DC695C7	SHA-1
5CE3CDFB61F3097E5974F5A07CF0BD2186585776	SHA-1
FAC3FB1C20F2A56887BDBA892E470700C76C81BA	SHA-1
AA374FA424CC31D2E5EC8ECE2BA745C28CB4E1E8	SHA-1
E50AD1A7A30A385A9D0A2C0A483D85D906EF4A9C	SHA-1
DC72D464289102CAAF47EC318B6110ED6AF7E5E4	SHA-1
9F7B4004018229FAD8489B17F60AADB3281D6177	SHA-1
2A2839F69EC1BA74853B11F8A8505F7086F1C07A	SHA-1
8EDB488B5F280490102241B56F1A8A71EBEEF8E3	SHA-1

MD5 Hashes

02f75c2b47b1733f1889d6bbc026157c
06cd99f0f9f152655469156059a8ea25
07e13b985c79ef10802e75aadfac6408
09350e100a4bda4a276fca6a968eb9ea
09745305cbad67b17346f0f6dba1e700

09924946b47ef078f7e9af4f4fcb59dc
09a77c0cb8137df82efc0de5c7fee46e
0abdaebbdbd5e6507e6db15f628d6fd7
0be6e64e2310e9a4f5782b9e98cdaf72
0d022eff24bc601d97d2088b4179bd18
16a278d0ec24458c8e47672529835117
17bc6f5b672b7e128cd5df51cdf10d37
183ad96b931733ad37bb627a958837db
198760a270a19091582a5bd841fbaec0
1bfbc0c9e0d9ceb5c3f4f6ced6bcfeae
1d0e79feb6d7ed23eb1bf7f257ce4fee
268dca9ad0dcb4d95f95a80ec621924f
2963cd266e54bd136a966bf491507bbf
2de01aac95f8703163da7633993fb447
2ef2703cfc9f6858ad9527588198b1b6
306310e0d2c0a497d968be1120b05143
35b07d0eddc357d7c388e819239595b2
38032a4d12d9e3029f00b120200e8e68
3b1dfeb298d0fb27c31944907d900c1d
3f051bb43a168e83c5ad222b324ebf68
3f326da2affb0f7f2a4c5c95ffc660cc
459593079763f4ae74986070f47452cf
474f08fb4a0b8c9e1b88349098de10b1
48405332ee067cdf29077b317dc7c555
490c885dc7ba0f32c07ddfe02a04bbb9
49c2821a940846bdacb8a3457be4663c
4e1b36182482644f5a377f3351f19118
4edc5d01076078906032f7299641f412
50e33e4d9229286e7d49c5b468fef285
578e5078ccb878f1aa9e309b4cfc2be5
579e45a09dc2370c71515bd0870b2078
5c2242b56a31d64b6ce82671d97a82a4
5d0ffbc8389f27b0649696f0ef5b3cfe
5ebfe9a9ab9c2c4b200508ae5d91f067
5fbfeec97e967325af49fa4f65bb2265
6eec1de7708020a25ee38a0822a59e88
712a8e4d3ce36d72ff74b785aaf18cb0
7413f08e12f7a4b48342a4b530c8b785
7937397e0a31cdc87f5b79074825e18e
7ead0113095bc6cb3b2d82f05fda25f3
82a52042008fc8313576bf5d4083abf4
8387ceba0c020a650e1add75d24967f2
85d316590edfb4212049c4490db08c4b
89081f2e14e9266de8c042629b764926
8b78558ff2731e8f0904f660a02813c0
8e9c5eca1726511e8710c9692127ca11
949e1e35e09b25fca3927d3878d72bf4

954f50301207c52e7616cc490b8b4d3c
9d1db33d89ce9d44354dcba9ebba4c2d
9ea365c1714eb500e5f4a749a3ed0fe7
a27a9324d282d920e495832933d486ee
ab7e59391ecf059f4394a22faabbbcb0
ad5485fac7fed74d112799600edb2fbf
afbcb626b770b1f87ff9b5721d2f3235
b135a56b0486eb4c85e304e636996ba1
b9be8d53542f5b4abad4687a891b1c03
bbd703f0d6b1cad4ff8f3d2ee3cc073c
c1364bbf63b3617b25b58209e4529d8c
c4141ee8e9594511f528862519480d36
c635e0aa816ba5fe6500ca9ecf34bd06
cb65d885f4799dbdf80af2214ecdc5fa
ce6e55abfe1e7767531eaf1036a5db3d
d4b4ba4615c5ff58c766b509c552ec9d
de991e1dc8de2510127dcf9919f58d8a
de991e1dc8de2510127dcf9919f58f8a
e29fe3c181ac9ddbb242688b151f3310
e62a52073fd7bfd251efca9906580839
e7aa0237fc3db67a96ebd877806a2c88
e7fc03267e47814e23e004e5f3a1205b
e87b575b2ddfb9d4d692e3b8627e3921
f01624ec3f19b171cee5250eec53ffc2
f2a0e9034d67f8200993c4fa8e4f5d15
f31ce3215945b7f5978404eca30bdfc8
f5e0f57684e9da7ef96dd459b554fded
f7de7d878835793ae439c5e551597b1e
fde55de117cc611826db0983bc054624

SHA-256 Hashes

11b5944715da95e4a57ea54968439d955114088222fd2032d4e0282d12a58abb
4216f63870e2cdfe499d09fce9caa301f9546f60a69c4032cb5fb6d5ceb9af32
5098ec21c88e14d9039d232106560b3c87487b51b40d6fef28254c37e4865182
660e60cc1fd3e155017848a1f6befc4a335825a6ae04f3416b9b148ff156d143
829eceee720b0a3e505efbd3262c387b92abdf46183d51a50489e2b157dac3b1
9d18defe7390c59a1473f79a2407d072a3f365de9834b8d8be25f7e35a76d818
c677a79b853d3858f8c8b86ccd8c76ebbd1508cc9550f1da2d30be491625b744
f14b1a91ed1ecd365088ba6de5846788f86689c6c2f2182855d5e0954d62af3b
a75886b016d84c3eaacaf01a3c61e04953a7a3adf38acf77a4a2e3a8f544f855
25d8ae4678c37251e7ffbaeddc252ae2530ef23f66e4c856d98ef60f399fa3dc
a4fb20b15efd72f983f0fb3325c0352d8a266a69bb5f6ca2eba0556c3e00bd15
68e6b9d71c727545095ea6376940027b61734af5c710b2985a628131e47c6af7
4c3499f3cc4a4fdc7e67417e055891c78540282dccc57e37a01167dfe351b244
586F30907C3849C363145BFDCDABE3E2E4688CBD5688FF968E984B201B474730
8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5
c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f
dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469
90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4
226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb
16F413862EFDA3ABA631D8A7AE2BFFF6D84ACD9F454A7ADAA518C7A8A6F375A5
05732E84DE58A3CC142535431B3AA04EFBE034CC96E837F93C360A6387D8FAAD
6FBB771CD168B5D076525805D010AE0CD73B39AB1F4E6693148FE18B8F73090B
912018AB3C6B16B39EE84F17745FF0C80A33CEE241013EC35D0281E40C0658D9
CAF6739D50366E18C855E2206A86F64DA90EC1CDF3E309AEB18AC22C6E28DC65
2963a90eb9e499258a67d8231a3124021b42e6c70dacd3aab36746e51e3ce37e
2AA1BBBE47F04627A8EA4E8718AD21F0D50ADF6A32BA4E6133EE46CE2CD13780
5A73FDD0C4D0DEEA80FA13121503B477597761D82CF2CFB0E9D8DF469357E3F8
C92C158D7C37FEA795114FA6491FE5F145AD2F8C08776B18AE79DB811E8E36A3

Mutex Name

Global\RRfreshRA_Mutex_Object

ECHO

CYBER THREAT INTELLIGENCE