GROUP-IB

THE BROTHERS GRIM

THE REVERSING TALE OF GRIMAGENT MALWARE USED BY RYUK

Albert Priego Bravo

Malware Analyst

|GROUP|IB|

Albert Priego, Malware Analyst at Group-IB

Albert is a skilled malware analyst and cyber threat intelligence expert who specializes in providing technical support for state-level investigations and working closely with Europol. Albert is an accomplished professional and holds many international certifications such as GIAC in Reverse Engineering Malware (GREM).

Group-IB at a Glance

GROUP|IB

450+

Enterprise customers
around the World

1300+

Successful Investigations
of Hi-tech Cybercrime Cases

70 000+

Hours of Hands-on
Incident Response

550+

Employees Worldwide

Recognized by Top Industry Experts

FORRESTER · IDC Analyze the Future · Gartner

Official Partner

Europol · Interpol

Recommended by

OSCE · SWIFT

Some of Our High-end Clients

Deutsche Bank · Raiffeisen Bank · Sony · Commonwealth Bank · Huawei

CERT-GIB

|GROUP|iB|

CERT-GIB (Computer Emergency Response Team) is a round-the-clock computer security incident response team

- ✓ Monitoring of incidents including the spread of malicious software and phishing
- ✓ Professional assistance from specialists with vast experience in response to cybercrimes
- ✓ Collection, analysis and preservation of digital evidences
- ✓ Prompt blocking of dangerous websites in the .RU and .PФ domains and more than 2,500 other domain zones
- ✓ Close cooperation with CERT teams, domain registrars, and hosting providers from all over the world
- ✓ 70 000+ hours of emergency incident response

Recognized as a competent organization of the Coordination Center for TLD RU (administrator of national top-level domains .RU and .PФ)

Accredited member of the international associations FIRST and Trusted Introducer

Member of OIC-CERT (Organization of the Islamic Cooperation-Computer Emergency Response Team)

Partner of IMPACT (International Multilateral Partnership Against Cyber Threats)

Member of APWG — Anti-Phishing Working Group

Ryuk gang

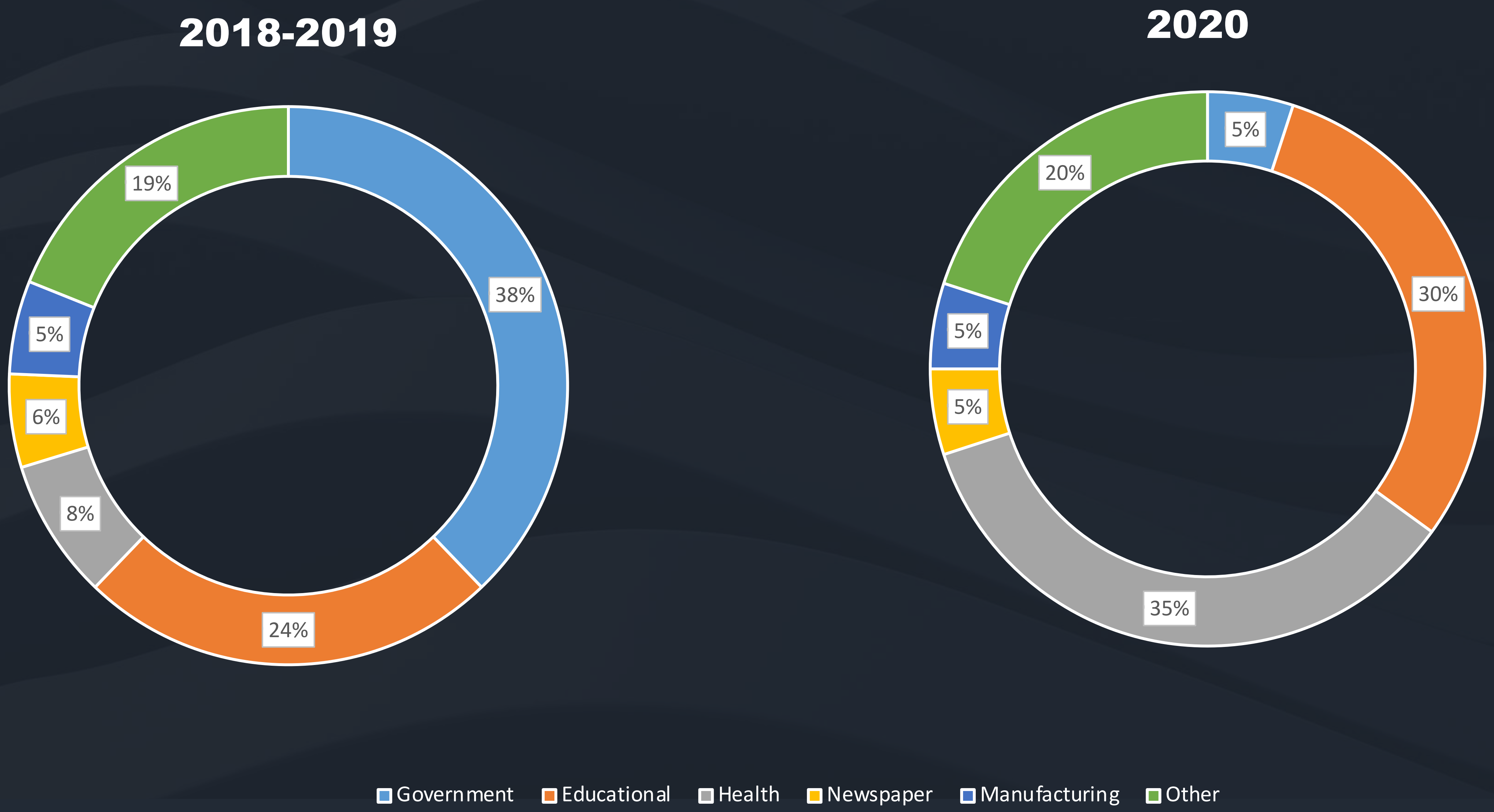
Ryuk Gang

- Appeared in August 2018
- Ryuk was built based on Hermes ransomware
- Linked to Wizard Spider and FIN6
- Delivered as a third-stage payload by using another malware
- Typical Ryuk killchains:
  - 2018-2019:
    - Phishing email -> Emotet -> Trickbot -> Ryuk
  - 2020:
    - SendGrid -> Google Drive link -> Bazar -> Trickbot -> Ryuk
    - SendGrid -> Google Drive link -> Bazar -> Cobalt Strike -> Ryuk
    - SendGrid -> Google Drive link -> Buer -> Cobalt Strike, SystemBC -> Ryuk
    - Phishing email -> Zloader -> Cobalt Strike -> Ryuk
- Latest malware added to their toolkit: **GrimAgent**

Ryuk targets

- Ryuk targeted companies and institutions from different sectors, for example:
  - Health (UHS hospitals, St. Lawrence Health System, Dickinson County Healthcare System)
  - Education (Baltimore County Public Schools)
  - Government (SEPE, Port Lavaca City Hall)
  - IT (Epiq Global, EVRAZ, Finastra, Sopra Steria)
  - Press (Tribune Publishing, Los Angeles Times, Tampa Bay Times)
  - Others: construction, law, R&D
- Recent Ryuk attacks:
  - Afnor
  - SEPE
  - Volue

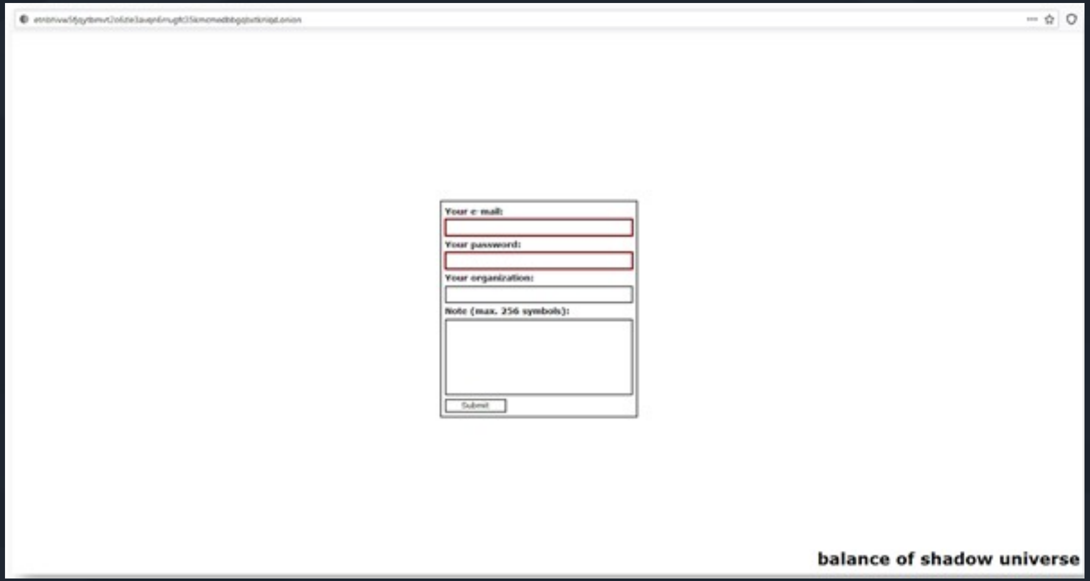
Targets


2018-2019
38%
24%
8%
6%
5%
19%
2020
5%
30%
35%
5%
5%
20%
Government
Educational
Health
Newspaper
Manufacturing
Other

GrimAgent

GrimAgent

- First version in the wild seen on August 9, 2020
- New malware used by Ryuk gang
- Prior stage of Ryuk ransomware
- Shared command and control



Your e-mail:

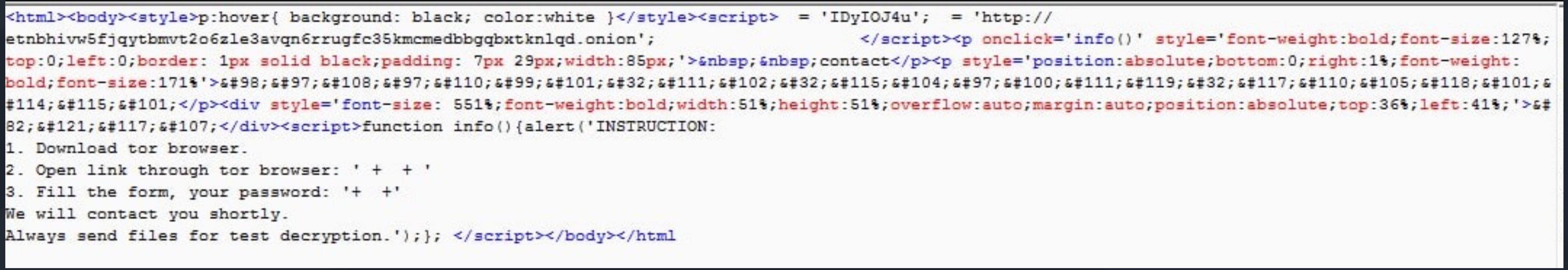
Your password:

Your organization:

Note (max. 256 symbols):

balance of shadow universe

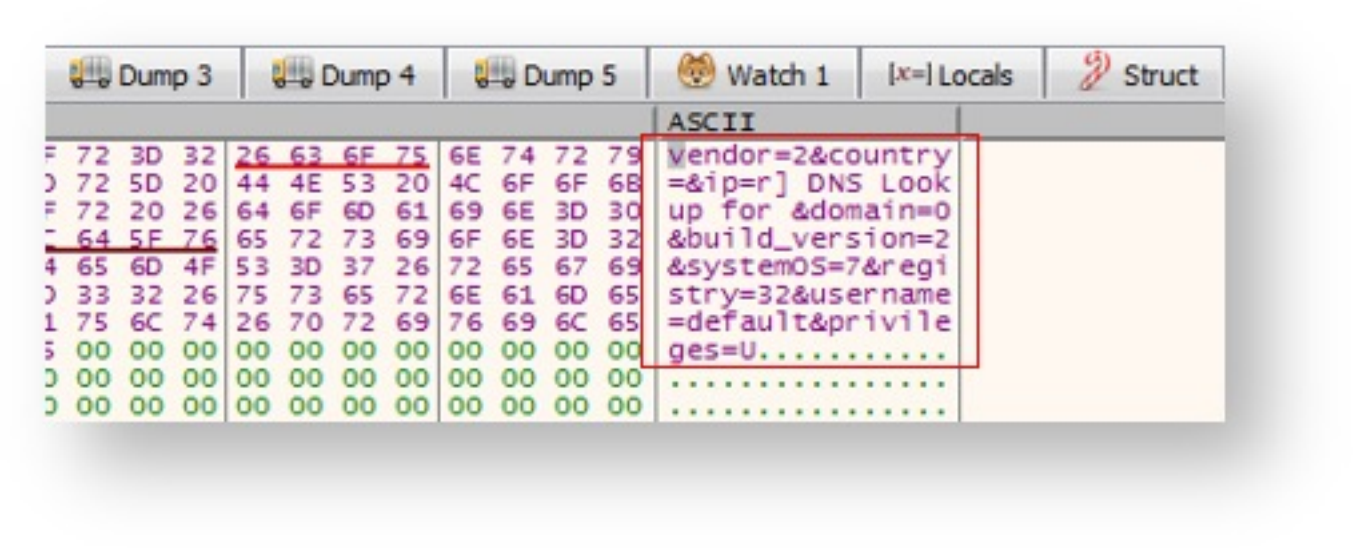
GrimAgent C2: hxxp://mirosoftplaymarket[.]top/gate.php
hxxp://mirosoftplaymarket[.]top:



```
<html><body><style>p:hover{ background: black; color:white }</style><script>  = 'IDyIOJ4u';  = 'http://
etnbhivw5fjqytbmvt2o6zle3avqn6rrugfc35kmcmedbbgqbxtknlqd.onion';                       </script><p onclick='info()' style='font-weight:bold;font-size:127%;
top:0;left:0;border: 1px solid black;padding: 7px 29px;width:85px;'>&nbsp;&nbsp;contact</p><p style='position:absolute;bottom:0;right:1%;font-weight:
bold;font-size:171%'>&#98;&#97;&#108;&#97;&#110;&#99;&#101;&#32;&#111;&#102;&#32;&#115;&#104;&#97;&#100;&#111;&#119;&#32;&#117;&#110;&#105;&#118;&#101;&
#114;&#115;&#101;</p><div style='font-size: 551%;font-weight:bold;width:51%;height:51%;overflow:auto;margin:auto;position:absolute;top:36%;left:41%;'>&#
82;&#121;&#117;&#107;</div><script>function info(){alert('INSTRUCTION:
1. Download tor browser.
2. Open link through tor browser: ' +  + '
3. Fill the form, your password: '+  +'
We will contact you shortly.
Always send files for test decryption.');}; </script></body></html
```

GrimAgent

- Defensive measures
- Retrieve information about the victim
  - IP and country code
  - Domain
  - Vendor
  - Build version
  - OS
  - Architecture
  - Username
  - Privileges
  - User_id
- Download and execute
- Update
- Execute DLL (MZ launcher trampoline)
- Symmetric and asymmetric encryption
- Execute
- Execute shellcode (MZ launcher)



```
                                                 ASCII
F 72 3D 32 26 63 6F 75 6E 74 72 79  vendor=2&country
D 72 5D 20 44 4E 53 20 4C 6F 6F 6B  =&ip=r] DNS Look
F 72 20 26 64 6F 6D 61 69 6E 3D 30  up for &domain=0
_ 64 5F 76 65 72 73 69 6F 6E 3D 32  &build_version=2
4 65 6D 4F 53 3D 37 26 72 65 67 69  &systemOS=7&regi
D 33 32 26 75 73 65 72 6E 61 6D 65  stry=32&username
1 75 6C 74 26 70 72 69 76 69 6C 65  =default&privile
5 00 00 00 00 00 00 00 00 00 00 00  ges=U...........
D 00 00 00 00 00 00 00 00 00 00 00  ................
D 00 00 00 00 00 00 00 00 00 00 00  ................
```

GrimAgent

Command list

Command ID	Functionality	Comments
1	Execute	Execute file through task scheduler
2	Execute Shellcode (MZ Launcher)	Parse shellcode, drop launcher and execute through task scheduler
3	Download and Execute (schtask)	Download from URI and execute
4	Update	Drops into the current directory and update the GrimAgent binary for the new one
5	Execute DLL (MZ Trampoline)	Download DLL from URI and execute it through MZ launcher
*6**	*Download and Execute (ShellExecuteW)*	*Download from URI and execute*

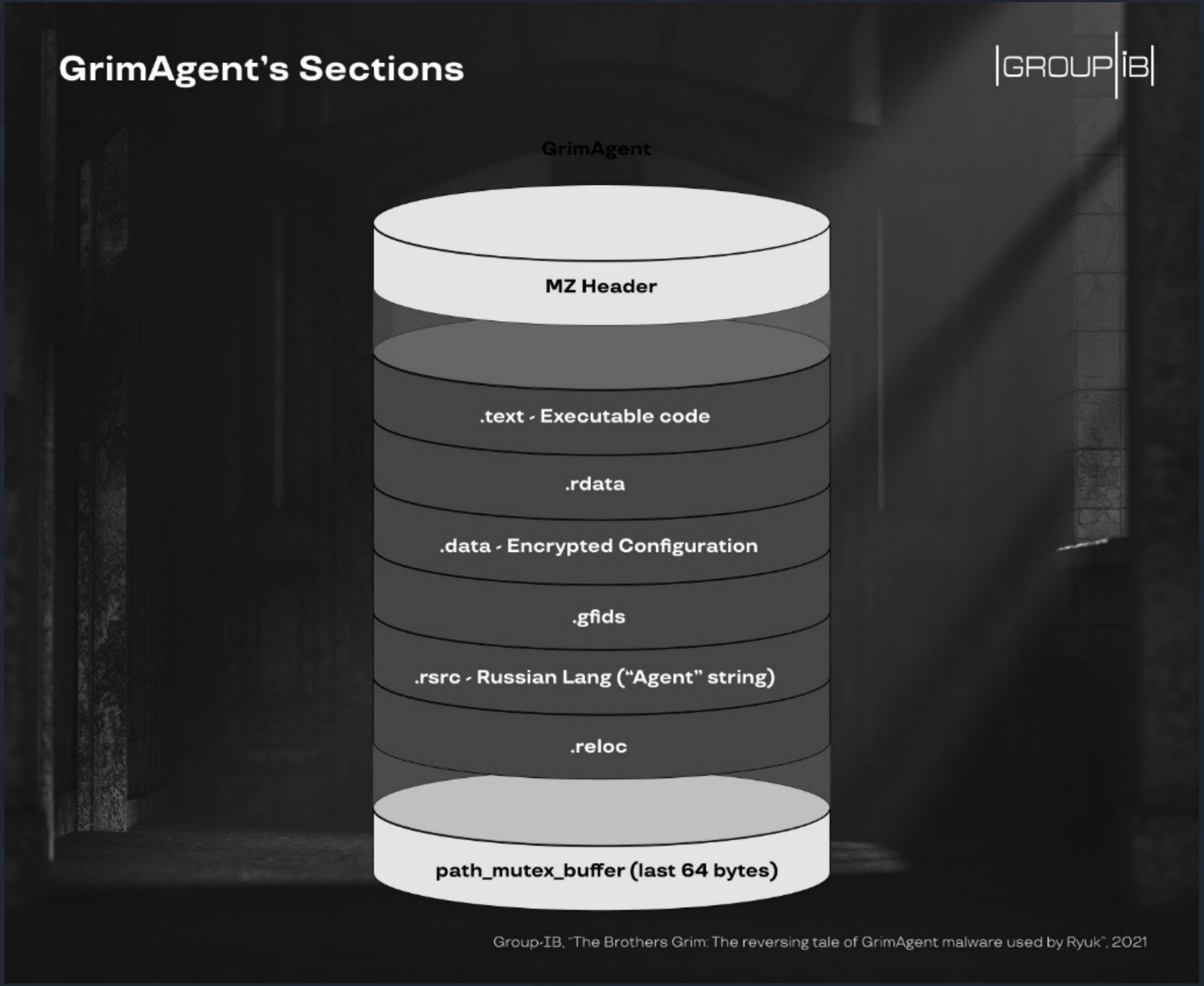
GrimAgent

Characteristics features

GrimAgent

Key Features

- Russian language inside .rsrc section
- Custom network protocol (bot-like)
- Symmetric and asymmetric encryption
- Usage of task scheduler and registry keys
- Writes 64 bytes in the end to compute Mutex name and define its configuration path
- Usage of embedded binaries (32b/64b) that act as a stepping stone for executing payloads
- Filtered payload delivery
- Under development



GrimAgent's Sections

GrimAgent

MZ Header

.text - Executable code

.rdata

.data - Encrypted Configuration

.gfids

.rsrc - Russian Lang ("Agent" string)

.reloc

path_mutex_buffer (last 64 bytes)

Group-IB, "The Brothers Grim: The reversing tale of GrimAgent malware used by Ryuk", 2021

GrimAgent

Updated Features

- Mutex creation and malware configuration path - Now is hardcoded in the sample
- Last 64 bytes (path_mutex_buffer) – Not used
- Updated persistence method - copies itself into a hardcoded path and sets persistence through Run key
- When the malware searched a writable directory, always created a file and wrote a random integer inside between 50 and 150 – Deleted
- Command 4 – Updated in newer versions
- Added Command 6 (execute through ShellExecuteW)

GrimAgent

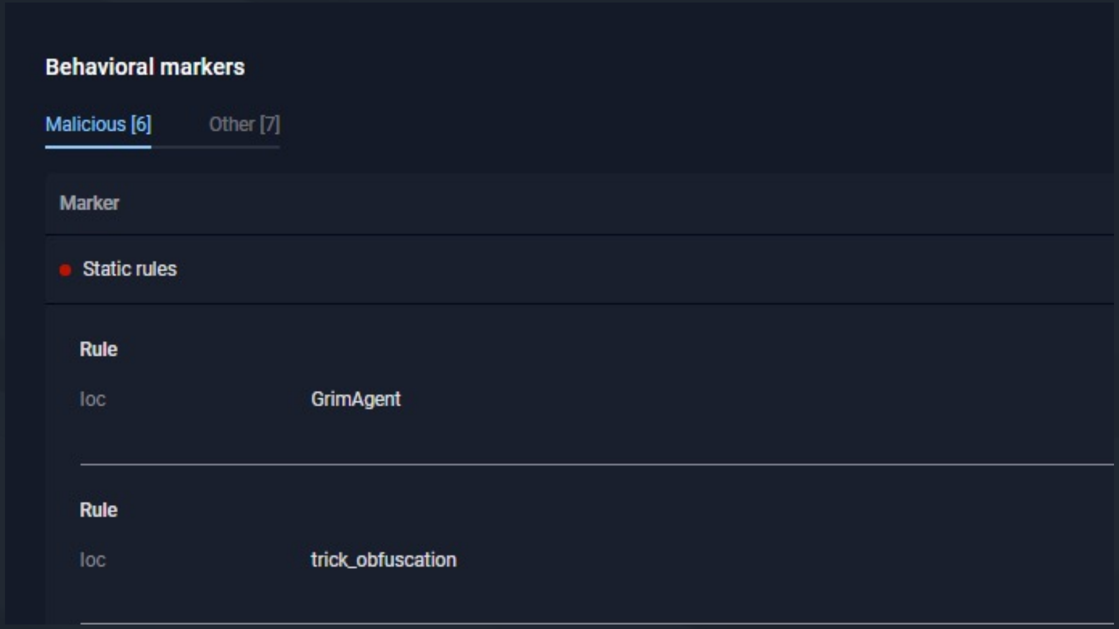
Detection Opportunities

Network communication & Threat Intel/Forensic usage

GrimAgent

Tracking and detecting the cyber threat

- Persistence - common path the malware uses is *C:/Users/Public*
- Mutex (old malware version)
- Network:
  - Request to *ip-api.com*
  - Common network path: */gate.php*
  - Request specific fields with refer to legitimate domains: google.com, youtube.com, etc
- Payload drop – embedded binary file
- Payload execution – scheduled tasks + ShellExecute



Behavioral markers

Marker

● Static rules

Rule	
loc	GrimAgent

Rule	
loc	trick_obfuscation

Link to rules: https://github.com/apriegob/GrimAgent/tree/main/Rules

GrimAgent

Client-server keys diagram

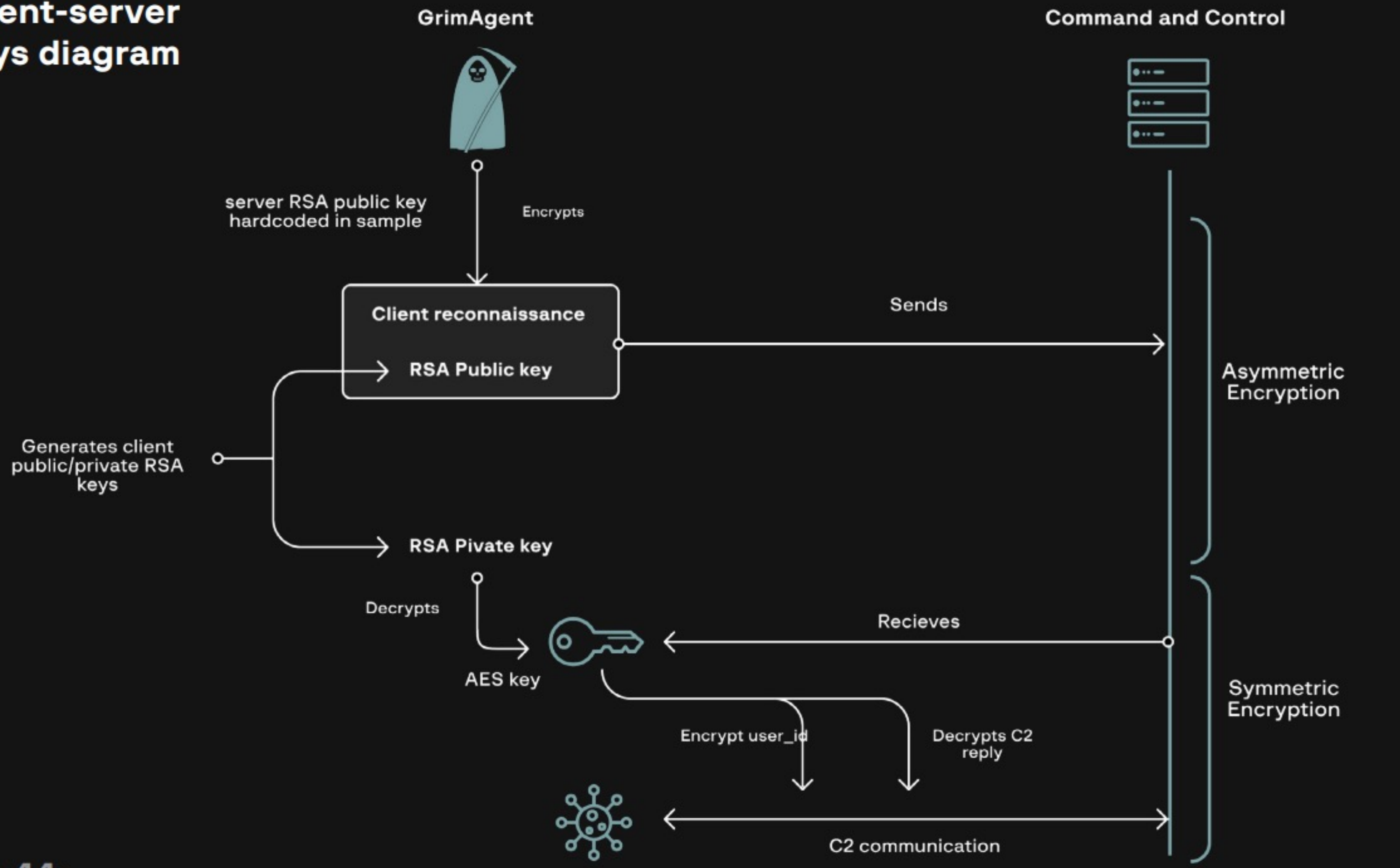


Fig 44:

GrimAgent

Honeypots and Forensic investigations

- Threat Intelligence based on honeypots:
  - Build custom honeypots in our DMZ in order to be infected with GrimAgent and check what happened by decrypting all commands and messages sent by the C2. This allows to get IOCs and new information of the malware.
- Forensic investigations:
  - Reconstruct what happened, how and what commands were executed with the full execution chain of the malware on the infected PC.

Only posible with the full understanding of how the malware works.

MITRE ATT&CK

Tactics	Technique	Sub-technique	Mitigations	Group-IB Solutions
Execution	Command and Scripting Interpreter - T1059	Windows Command Shell - T1059.003	Execution Prevention (M1038)	Threat Hunting Framework
	Native API - T1106		Execution Prevention (M1038)	
	Scheduled Task/Job - T1053	Scheduled Task - T1053.005	Audit (M1047), Operating System Configuration (M1028), Privileged Account Management (M1026), User Account Management (M1018)	
Persistence	Boot or Logon Autostart Execution- T1547	Registry Run Keys / Startup Folder - T1547.001		Threat Hunting Framework
	Scheduled Task/Job - T1053	Scheduled Task - T1053.005	Audit (M1047), Operating System Configuration (M1028), Privileged Account Management (M1026), User Account Management (M1018)	
Privilege Escalation	Scheduled Task/Job - T1053	Scheduled Task - T1053.005	Audit (M1047), Operating System Configuration (M1028), Privileged Account Management (M1026), User Account Management (M1018)	Threat Hunting Framework
Defense Evasion	Deobfuscate/Decode Files or Information - T1140			Threat Hunting Framework
	Indirect Command Execution - T1202			
	Masquerading - T1036	Masquerade Task or Service – T1036.004		
		Match Legitimate Name or Location – T1036.005	Code Signing (M1045), Execution Prevention (M1038), Restrict File and Directory Permissions (M1022)	
	Obfuscated Files or Information - T1027	Binary Padding - T1027.001		
		Software Packing - T1027.002	Antivirus/Antimalware (M1049)	
	Virtualization/Sandbox Evasion - T1497	Time Based Evasion - T1497.003		
Command and Control	Application Layer Protocol - T1071	Web Protocols - T1071.001	Network Intrusion Prevention (M1031)	Threat Hunting Framework
	Data Encoding - T1132	Standard Encoding - T1132.001	Network Intrusion Prevention (M1031)	
	Data Obfuscation - T1001	Junk Data - T1001.001	Network Intrusion Prevention (M1031)	
	Encrypted Channel - T1573	Symmetric Cryptography - T1573.001	Network Intrusion Prevention (M1031)	
		Asymmetric Cryptography - T1573.002	Network Intrusion Prevention (M1031), SSL/TLS Inspection (M1020)	
	Fallback Channels - T1008		Network Intrusion Prevention (M1031)	
	Ingress Tool Transfer - T1105		Network Intrusion Prevention (M1031)	
	Multi-Stage Channels - T1104		Network Intrusion Prevention (M1031)	
Collection	Archive Collected Data – T1560	Archive via Custom Method – T1560.003		Threat Hunting Framework
Exfiltration	Exfiltration Over C2 Channel - T1041		Network Intrusion Prevention (M1031)	Threat Hunting Framework
Impact	Data Encrypted for Impact - T1486		Data Backup (M1053)	Threat Hunting Framework

CONCLUSION

Hunt or be Hunted

We are facing a powerful and skillful adversary that has affected worldwide companies asking for large sums of money. They continue to evolve and create new, better and more sophisticated tools for their attacks.

Their techniques, tactics, and procedures improve. From the defense and intelligence side, we must continue to advance and share knowledge in order to anticipate their intrusions before it is too late.

I recommend to read the full article or, at least the condensed version where the threat is fully explained as well as different Yara and Suricata rules for its detection and containment.

Link: https://blog.group-ib.com/grimagent

THE BROTHERS GRIM

→ GROUP-IB

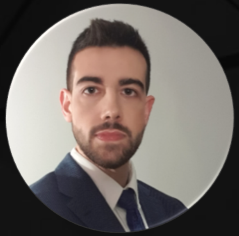
JULY 2021

THE REVERSING TALE OF GRIMAGENT MALWARE USED BY RYUK

GROUP-IB

group-ib.com

Preventing and investigating cybercrime since 2003



Albert Priego Bravo

Malware Analyst

www.group-ib.com

group-ib.com/blog

info@group-ib.com

+65 3159-3798

twitter.com/GroupIB_GIB

facebook.com/groupibHQ

linkedin.com/organization/1382013

instagram.com/group_ib