GLOBAL CYBER SECURITY COMPANY · GIB · GLOBAL CYBER SECURITY COMPANY

Whitepaper

# THE EVOLUTION OF RANSOMWARE AND ITS DISTRIBUTION METHODS

group-ib.com

GROUP-IB

# CONTENT

# Introduction

The most massive ransomware attacks, such as **“WannaCry”**, **“NotPetya”** and **“Bad Rabbit”**, died down in 2017. However, despite the reduced threat level, this type of malware remains one of the most common cyber threats in 2018. Like many other threats, malware evolves over time. Modern ransomware makes it impossible to decrypt data without the relevant decryption key, and its distributors not only intend to infect victims with malware once, but also to study their IT infrastructure for future targeted attacks. In most cases, this means espionage or data theft.

According to the findings of Group-IB’s digital forensic experts, hackers most commonly spread ransomware by stealing administrator credentials and then using RDP tools to execute the malware directly on the remote machine.

However, attackers also spread ransomware using more traditional techniques like spear phishing. Password-protected attachments have become another popular strategy, and exploit kits like RIG and GrandSoft are also frequently used.

We are also aware of infection cases in which ransom was not the main objective – for example, banking Trojans.

This analytical report presents some technical details of ransomware attacks we have investigated, and provides basic recommendations for preventing such incidents.

**300 000+**

number of devices
compromised by WannaCry

**200+**

countries suffered
from WannaCry attacks

**80+**

companies were victims
of NotPetya cyberattacks

# What is ransomware?

**Ransomware is a form of malware that uses algorithms to encrypt a user’s files so that they cannot be accessed without a decryption key.**

The attackers offer this key in exchange for cryptocurrency. The amount is defined in instruction files generated by the malware.

That said, the attackers might significantly reduce the ransom amount in the course of negotiations.

It is worth noting that the scammers’ goal is not always ransom. We have also observed cases in which ransomware was distributed across a compromised IT infrastructure in order to cover the tracks of a targeted attack.

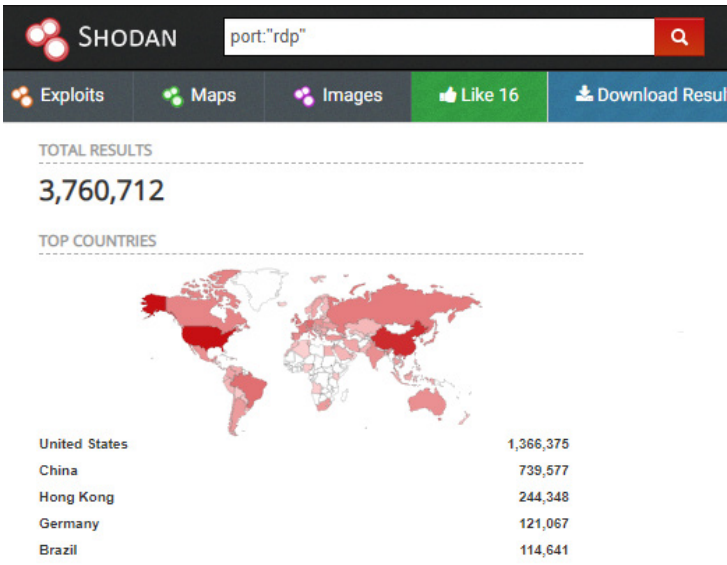
# How ransomware is spread

## Compromising servers with RDP

Our experience is that, despite its primitiveness, this has become the type of attack most often used by scammers in 2018.

Many system administrators leave the RDP port (3389) on servers open to facilitate their work, and allow them access to these machines anywhere and at any time. That said, the standard administrator account is sometimes not blocked even if it is not being used, which makes it much easier for attackers to perform brute-force attacks — they already know the login.

**3 500 000+** systems with an available port 3389 in Shodan



port:"rdp"

TOTAL RESULTS

3,760,712

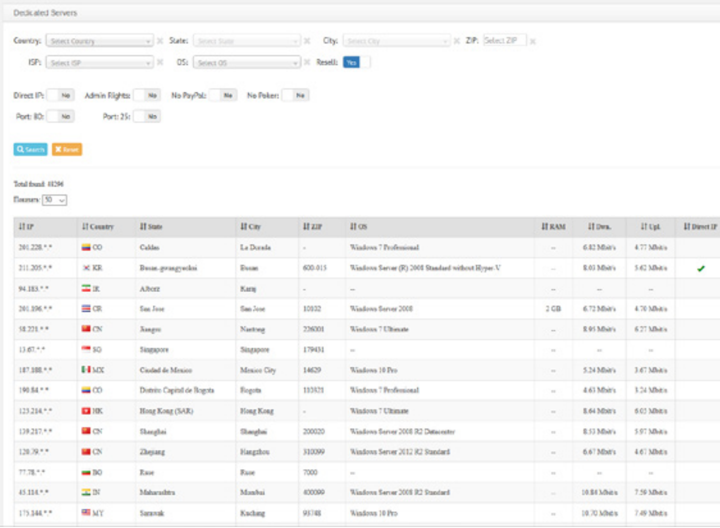
TOP COUNTRIES

| | |
|---|---|
| United States | 1,366,375 |
| China | 739,577 |
| Hong Kong | 244,348 |
| Germany | 121,067 |
| Brazil | 114,641 |

Figure 1. Shodan search results

Often, ransomware distributors need not even carry out a password attack to gain access to such a server – everything has already been done for them. On underground resources such as "xDedic" and "UAS RDP Shop", for example, access to one of thousands of compromised servers can be purchased for just a few dollars.

Once attackers gain access to a server, they can either run the ransomware immediately, or else attempt to propagate across the network, perform reconnaissance, and run the malware on a massive scale. They can also adjust their ransom request to reflect the value of a workstation or server. In addition, attackers can create new access channels to ensure that the infrastructure can be compromised again.



Dedicated Servers

Country: Select Country State: Select State City: Select City ZIP: Select ZIP
ISP: Select ISP OS: Select OS Resell: Yes

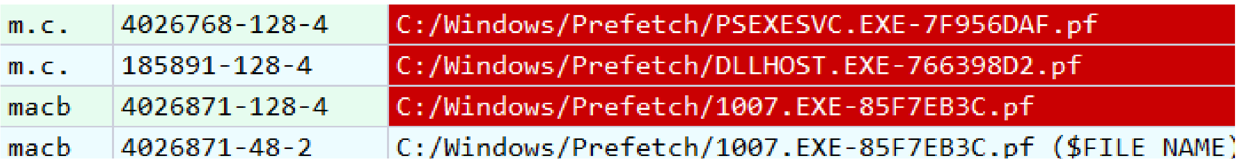
Direct IP: No Admin Rights: No No PayPal: No No Poker: No
Port: 80: No Port: 25: No

Total found: 41296
[illegible]: 50

| IP | Country | State | City | ZIP | OS | RAM | Dwn. | Upl. | Direct IP |
|---|---|---|---|---|---|---|---|---|---|
| 201.228.*.* | CO | Caldas | La Dorada | - | Windows 7 Professional | – | 6.82 Mbit/s | 4.77 Mbit/s | |
| 211.205.*.* | KR | Busan-gwangyeoksi | Busan | 600-015 | Windows Server (R) 2008 Standard without Hyper-V | – | 8.03 Mbit/s | 5.62 Mbit/s | ✓ |
| 94.183.*.* | IR | Alborz | Karaj | - | – | – | – | – | |
| 201.196.*.* | CR | San Jose | San Jose | 10032 | Windows Server 2008 | 2 GB | 6.72 Mbit/s | 4.70 Mbit/s | |
| 58.221.*.* | CN | Jiangsu | Nantong | 226001 | Windows 7 Ultimate | – | 8.95 Mbit/s | 6.27 Mbit/s | |
| 13.67.*.* | SG | Singapore | Singapore | 179431 | – | – | – | – | |
| 187.188.*.* | MX | Ciudad de Mexico | Mexico City | 14629 | Windows 10 Pro | – | 5.24 Mbit/s | 3.67 Mbit/s | |
| 190.84.*.* | CO | Distrito Capital de Bogota | Bogota | 110321 | Windows 7 Professional | – | 4.63 Mbit/s | 3.24 Mbit/s | |
| 123.214.*.* | HK | Hong Kong (SAR) | Hong Kong | - | Windows 7 Ultimate | – | 8.64 Mbit/s | 6.05 Mbit/s | |
| 139.217.*.* | CN | Shanghai | Shanghai | 200020 | Windows Server 2008 R2 Datacenter | – | 8.53 Mbit/s | 5.97 Mbit/s | |
| 120.79.*.* | CN | Zhejiang | Hangzhou | 310099 | Windows Server 2012 R2 Standard | – | 6.67 Mbit/s | 4.67 Mbit/s | |
| 77.78.*.* | BG | Ruse | Ruse | 7000 | – | – | – | – | |
| 45.114.*.* | IN | Maharashtra | Mumbai | 400099 | Windows Server 2008 R2 Standard | – | 10.84 Mbit/s | 7.59 Mbit/s | |
| 175.144.*.* | MY | Sarawak | Kuching | 93748 | Windows 10 Pro | – | 10.70 Mbit/s | 7.49 Mbit/s | |

Figure 2. Access to servers for sale on "UAS RDP Shop"

Attackers frequently use **the “PsExec” tool** of the “Windows Sysinternals” package to deliver and download ransomware on all available systems.

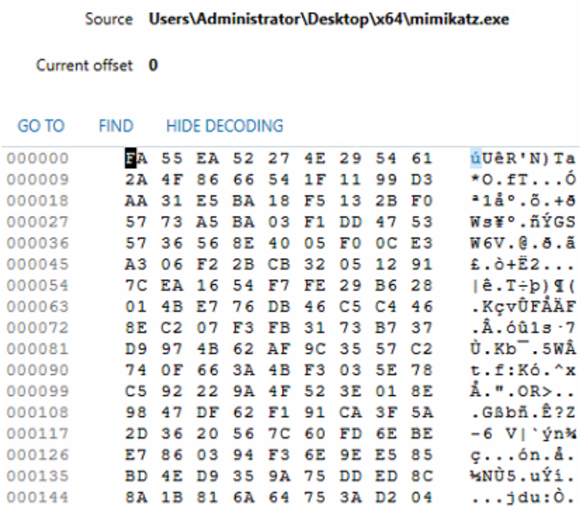


| | | |
|---|---|---|
| m.c. | 4026768-128-4 | C:/Windows/Prefetch/PSEXESVC.EXE-7F956DAF.pf |
| m.c. | 185891-128-4 | C:/Windows/Prefetch/DLLHOST.EXE-766398D2.pf |
| macb | 4026871-128-4 | C:/Windows/Prefetch/1007.EXE-85F7EB3C.pf |
| macb | 4026871-48-2 | C:/Windows/Prefetch/1007.EXE-85F7EB3C.pf ($FILE NAME) |

Figure 3. Prefetch files illustrating the launch of “PsExec”, followed by the launch of “1007.exe”

The attackers often use the **“Mimikatz”** tool to steal authorized users’ passwords and hashes which are stored in the memory of the compromised server. They can then access other systems on the network using the same RDP.

It is worth noting that in most cases it is possible to establish the fact of using this utility only by the file name. It is not possible to restore the original file content due to encryption.



Source Users\Administrator\Desktop\x64\mimikatz.exe

Current offset 0

```
000000   FA 55 EA 52 27 4E 29 54 61   úUêR'N)Ta
000009   2A 4F 86 66 54 1F 11 99 D3   *O.fT...Ó
000018   AA 31 E5 BA 18 F5 13 2B F0   ª1å°.õ.+ð
000027   57 73 A5 BA 03 F1 DD 47 53   Ws¥°.ñÝGS
000036   57 36 56 8E 40 05 F0 0C E3   W6V.@.ð.ã
000045   A3 06 F2 2B CB 32 05 12 91   £.ò+Ë2...
000054   7C EA 16 54 F7 FE 29 B6 28   |ê.T÷þ)¶(
000063   01 4B E7 76 DB 46 C5 C4 46   .KçvÛFÅÄF
000072   8E C2 07 F3 FB 31 73 B7 37   .Â.óû1s·7
000081   D9 97 4B 62 AF 9C 35 57 C2   Ù.Kb¯.5WÂ
000090   74 0F 66 3A 4B F3 03 5E 78   t.f:Kó.^x
000099   C5 92 22 9A 4F 52 3E 01 8E   Å.".OR>..
000108   98 47 DF 62 F1 91 CA 3F 5A   .Gßbñ.Ê?Z
000117   2D 36 20 56 7C 60 FD 6E BE   -6 V|`ýn¾
000126   E7 86 03 94 F3 6E 9E E5 85   ç...ón.å.
000135   BD 4E D9 35 9A 75 DD ED 8C   ½NÙ5.uÝí.
000144   8A 1B 81 6A 64 75 3A D2 04   ...jdu:Ò.
```

Figure 4. The file “mimikatz.exe” infected by encryption ransomware

According to our data, in 2018 RDP attacks were most often used to download the **ransomware “GlobeImposter”**, first discovered in December 2017.

“GlobeImposter” uses an RSA 2048-bit key to encrypt files. It saves part of the key-related data in a newly created file named «%AllUserProfile%\Public\.

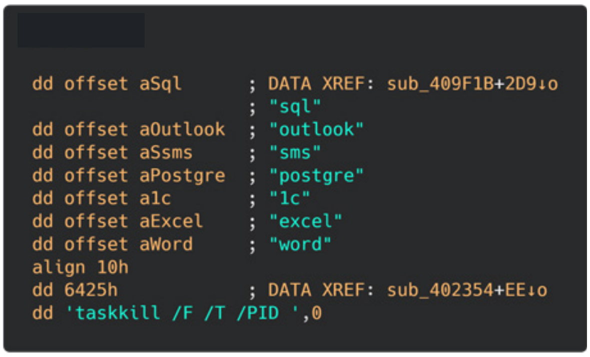
Before it starts encrypting files, “GlobeImposter” searches for running processes whose names include special keywords and kill them afterwards.

**Doing so allows the ransomware to access the “SQL”, “Outlook”, “PostgreSQL”, and “1C” databases, as well as Word documents and Excel tables that were open at the time of launch.**

**Keywords**

SQL Outlook SSMS 1C

Postgre Excel Word

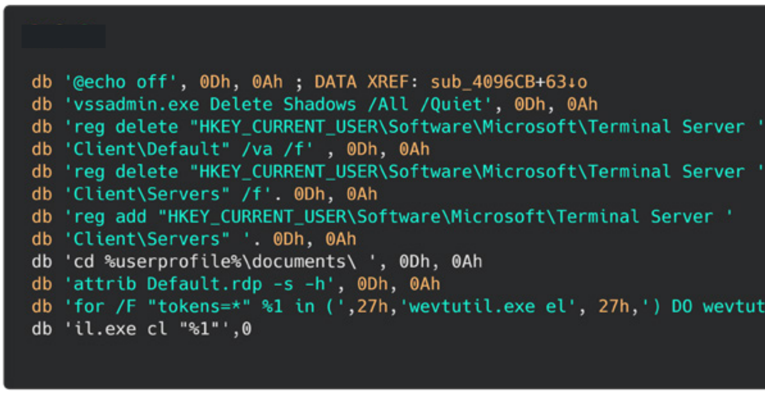


```
dd offset aSql      ; DATA XREF: sub_409F1B+2D9↓o
                    ; "sql"
dd offset aOutlook  ; "outlook"
dd offset aSsms     ; "sms"
dd offset aPostgre  ; "postgre"
dd offset a1c       ; "1c"
dd offset aExcel    ; "excel"
dd offset aWord     ; "word"
align 10h
dd 6425h            ; DATA XREF: sub_402354+EE↓o
dd 'taskkill /F /T /PID ',0
```

Figure 5. Keywords search

To cover its tracks and prevent the victim from restoring encrypted files, the malware creates and executes a batch file that deletes backups from shadow copies, removes Remote Desktop information and clears event logs.

**The specified script will be automatically restarted after the completion of the encryption process.**

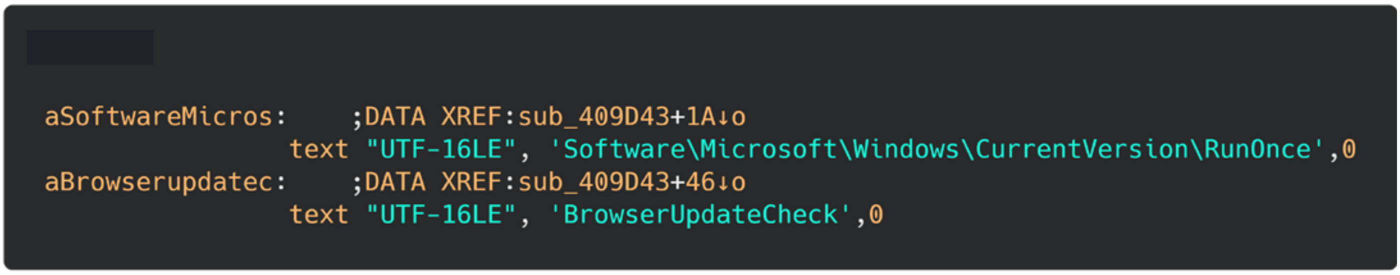


```
[redacted]

db '@echo off', 0Dh, 0Ah ; DATA XREF: sub_4096CB+63↓o
db 'vssadmin.exe Delete Shadows /All /Quiet', 0Dh, 0Ah
db 'reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server '
db 'Client\Default" /va /f' , 0Dh, 0Ah
db 'reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server '
db 'Client\Servers" /f'. 0Dh, 0Ah
db 'reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server '
db 'Client\Servers" '. 0Dh, 0Ah
db 'cd %userprofile%\documents\ ', 0Dh, 0Ah
db 'attrib Default.rdp -s -h', 0Dh, 0Ah
db 'for /F "tokens=*" %1 in (',27h,'wevtutil.exe el', 27h,') DO wevtut
db 'il.exe cl "%1"',0
```

To ensure its autorun after the reboot of the affected computer, “GlobeImposter” creates a parameter in the registry key “HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce”, which includes the path to a copy of the executed file.

**Each directory with encrypted files is supplemented with the file “how_to_back_files.html”, which contains instructions for making a payment in order to decrypt the files.**



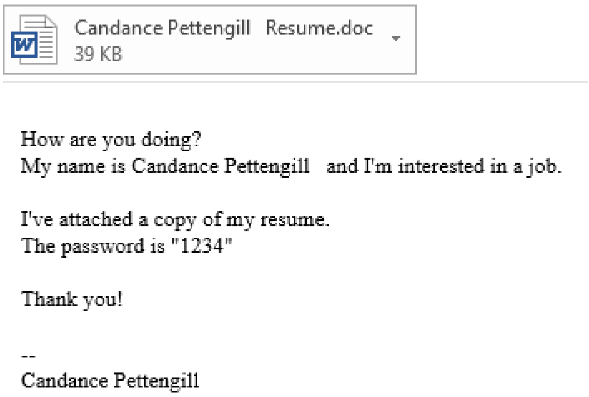
```
[redacted]

aSoftwareMicros:     ;DATA XREF:sub_409D43+1A↓o
                text "UTF-16LE", 'Software\Microsoft\Windows\CurrentVersion\RunOnce',0
aBrowserupdatec:     ;DATA XREF:sub_409D43+46↓o
                text "UTF-16LE", 'BrowserUpdateCheck',0
```

## Phishing campaigns

It is typical for many types of malware to be distributed using phishing emails, and ransomware is no exception. In 2018, phishing emails were usually used to spread “GandCrab”, “GlobeImposter”, “Hermes”, and “Sigma” malware. Attackers’ favourite tool is a password-protected Microsoft Word document.

The ransomware requires action from the user, enabling malware to be downloaded and executed:



Candance Pettengill Resume.doc
39 KB

How are you doing?
My name is Candance Pettengill and I'm interested in a job.

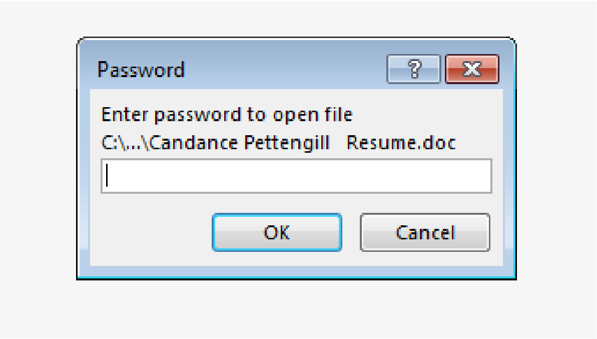
I've attached a copy of my resume.
The password is "1234"

Thank you!

--
Candance Pettengill

An email with a malicious attachment, which was sent out on October 24th, 2018.

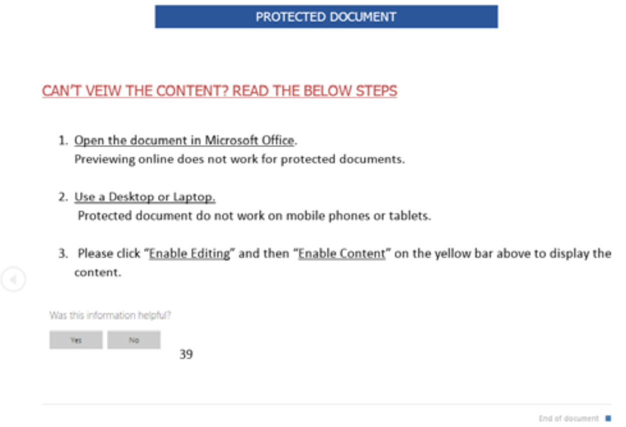
**1** **First, they must open the file and enter the password indicated in the body of the letter:**



Password

Enter password to open file
C:\...\Candance Pettengill Resume.doc

**2** **Second, they must enable blocked content, which will start the macro:**



PROTECTED DOCUMENT

CAN’T VEIW THE CONTENT? READ THE BELOW STEPS

1. Open the document in Microsoft Office.
   Previewing online does not work for protected documents.
2. Use a Desktop or Laptop.
   Protected document do not work on mobile phones or tablets.
3. Please click “Enable Editing” and then “Enable Content” on the yellow bar above to display the content.

Was this information helpful?

**This causes the ransomware to be downloaded from the attackers’ IP address, saved to the “Temp” directory and executed.**

## Exploit kits and other malware

Attackers have used exploit kits ranging from the very old (e.g. “GrandSoft”) to the relatively new (e.g. “RIG”) to deliver some types of ransomware like “GandCrab”. These exploit kits allow attackers to distribute ransomware through compromised websites. They are able to collect information about victims’ computers, select an exploit based on the vulnerabilities they detect, and ultimately download and execute the malware.

Additionally, this year some well-known banking Trojans (in particular “Emotet” and “Trickbot”) appeared to distribute ransomware such as “Ryuk” and “BitPaymer”.

These Trojans have a modular architecture, allowing them to expand their capabilities to include network distribution, exploitation of known vulnerabilities, and user password theft. This not only exposes attacked IT infrastructure to loss of access to data, but allows attackers to fully control it, allowing them to spread the infection or carry out other illegal actions like data theft.

# Group-IB case study: Infection with «GlobeImposter»

**Client profile**

A large development company whose IT infrastructure includes more than 400 workstations and servers

### Situation:

Threat actors gained access to the company’s server via RDP and compromised an administrative account, which enabled them to spread the GlobeImposter ransomware. Moreover, the hackers installed the remote control software TeamViewer on servers on which the malware was not launched.

### Action:

As part of incident response activities, Group-IB’s Forensic Lab specialists identified the compromised server (i.e. the malware entry point) and all infected workstations and servers. Furthermore, thanks to rapid forensic analysis, our specialists determined on which servers the attackers installed the remote control software.

### Results

- The client obtained comprehensive information about the incident, which will help the company protect itself against such threats in the future.
- Responding to the incident correctly made it possible to cut off the attackers from the infrastructure completely and prevent further intrusions and leaks of confidential information.
- The client received detailed recommendations on how to increase the security of the company’s IT infrastructure.

# Recommendations for preventing ransomware attacks

1 Use VPN whenever accessing servers through RDP.

2 If it is not possible to use VPN, implement multi-factor authentication.

3 Block accounts after a certain number of failed login attempts within a short period of time.

4 Ensure that the password of the account used for access via RDP is complex, and change it regularly.

5 Use NLA (Network Level Authentication) for RDP connections.

6 Enable TLS (Transport Layer Security) for RDP connections.

7 Change the default port (3389).

8 Restrict the list of IP addresses that can be used to make RDP connections.

9 Install anti-spam and anti-phishing filters.

10 Regularly update anti-virus protection, and audit the work logs of your protection software.

11 Implement a sandbox solution to detect malware not detected by antivirus software.

12 Perform timely updates of operating systems and application software.

# Polygon from Group-IB Threat Hunting Framework

## Prevention of ransomware attacks

**Polygon** – sophisticated sandboxing technology performing advanced behavioural files analysis in an isolated environment. AI-powered detection of previously unknown malicious code, which is not detected by antivirus software and signature-based systems.

Can be deployed in inline mode to block incoming emails with malicious attachments and prevent malware infection or data loss.

### Be a step ahead of attackers

With over 17 years of threat research and analysis, we possess unparalled expertise and state-of-the-art tools for pattern recognition in adversaries' TTPs.

A synergy with Group-IB's proprietary Threat Intelligence system allows getting unique data about new threats and promptly upgrading detection rules accordingly.

**Group-IB is ranked among the best threat intelligence vendors in the world by**

IDC | GARTNER
FORRESTER

## How Polygon works

### Object extraction

- Email attachments
- Files from web traffic
- Links

### Launch in an isolated environment

- Real-live emulation of end user environment
- Detection of sandbox bypassing techniques

### Behaviour analysis

In-depth analysis of suspicious files behaviour

### Detailed report

Containing network activity, process tree, video cast

### Extraction of additional IoCs

Full context to trigger threat hunting across the network

**Blocking in inline mode**

**Notification in monitoring mode**

Learn more about
**Threat Hunting Framework**

group-ib.com/threat-hunting-framework

# Group-IB's response to ransomware

Access to the data on a device infected with ransomware cannot be restored without decryption tools, and it is not recommended to pay ransom to the attackers.

**Still, Group-IB experts believe that the response to such ransomware is extremely important.**

A professional response to ransomware allows you to:

- **Minimize damage**
- **Clean the infrastructure in order to prevent similar incidents in the future, including detection of "sleeping" backdoors**
- **Gather all necessary information for creating a list of Indicators of Compromise**
- **Collect an evidence base, as well as information necessary for the investigation**
- **Get recommendations on enhancing information security level of infrastructure and personnel**

## Stages of Group-IB incident response

### 1 Network traffic analysis

Implementation of Group-IB Threat Hunting Framework Huntbox allows the response team to:

- **Monitor network traffic**
- **Detect suspicious communications that cannot be detected by signature-based security systems**
- **Analyze and block data on end devices**

### 2 Forensic analysis

A rapid forensic analysis of workstations and servers used by attackers to compromise of the IT infrastructure is carried out in order to identify:

- **Where the compromise began**
- **How the attackers moved across the network**
- **What tools they used**
- **What vulnerabilities have been exploited**

### 3 Malware analysis

Digital forensic laboratory specialists conduct basic or advanced static and dynamic analysis of malicious code detected during the incident response, which allows them to:

- **Detect tracks quickly and efficiently**
- **Keep malicious code from becoming fixed in systems, while preventing re-infection of infrastructure**
- **Neutralize threats that have already spread and become entrenched**

**Once this work has been completed, Group-IB experts prepare a detailed report describing the incident as well as a set of recommendations for improving infrastructure security. This minimizes the risk of similar incidents in the future.**

# About Group-IB

**Group-IB is one of the world's leading developers of solutions for cyber-attack detection and prevention, fraud detection, and protection of intellectual property online.**

**17**
years of hands-on experience

**1,200+**
cybercrime investigations worldwide

**$300 mln**
was returned to a client company as the result of our efforts

**65, 000+**
hours of incident response

Group-IB's security ecosystem provides automated tracking of malicious activities, extraction and analysis of threat data, mapping of adversaries' infrastructure and enrichment of their profiles. Our top-tier experts relentlessly reinforces our technologies with insights "from the battlefield".

## Group-IB Products

- **Threat Intelligence & Attribution**
- **Threat Hunting Framework**
- **Fraund Hunting Platform**
- **Digital Risk Protection**

INTERPOL | EUROPOL

**Official Europol and Interpol partner**

IDC | GARTNER | FORRESTER

**Group-IB is ranked among the best Threat Intelligence vendors in the world, according to IDC, Gartner and Forrester**

OSCE

**Recommended by the Organization for Security and Co-operation in Europe (OSCE)**

### PREVENTION

- Penetration Testing
- Red Teaming
- Security Assessment
- Incident Response Readiness Assessment (Pre-IR)
- Compromise Assessment
- Compliance Audit

### RESPONSE

- Incident Response Retainer
- 24/7 CERT-GIB
- Incident Response

### INVESTIGATION

- Digital Forensics
- Investigation
- eDiscovery
- Financial Forensics

### EDUCATION

- Incident Responder
- Malware Analyst
- Digital Forensics Analyst
- Threat Hunter

## Contact us to learn more

info@group-ib.com www.group-ib.com

GROUP|IB