Executive summary

Incident Response statistics are based on IR retainer services and IR fireman services for organizations contacting us during an incident.

Threat intelligence view

- Initial attack vector
  - 37% Vulnerability exploitation
  - 30% Malicious e-mail
  - 13% Brute-force

- Impact
  - Threat hunting with rich telemetry and specifically deep tracing of PowerShell is a must to be able to detect attacks
  - PsExec is not a suspicious event, but an incident to manage
  - 34% Ransomware
  - 21% Malware infection
  - 8% Data leakage
  - 9% Money theft

- Move around and get things done
  - 25% PowerShell
  - 22% PsExec
  - 14% Network Scanner
  - 8% ProcDump

- Exercise pace of security operations as it matters for Ransomware
  - Backup your data frequently and on separated infrastructure

Security operations metrics view

- Attack duration
  - 31% days
  - 24% weeks
  - 22% months
  - 13% hours
  - Most of fast detection times are related to visible infrastructure or process disruptions from Ransomware

- Detection reason
  - 32% suspicious file
  - 27% files encrypted
  - 13% suspicious endpoint activity
  - 11% other security tool alert
  - Security operations and toolstacks play a big role in incident identification

- Remediation duration
  - 43% weeks
  - 27% months
  - 15% hours
  - There is always room for improvement. Stick with IR retainer or prepare a list of IR providers and exercise with them
Introduction

The Incident Response Analyst Report provides insights into incident investigation services conducted by Kaspersky in 2019. We deliver a range of services to help organizations when they are in need: incident response, digital forensics and malware analysis. Data in the report comes from our daily practices with organizations seeking assistance with full-blown incident response or complimentary expert activities for their internal incident response teams.

Geography of incident responses

Kaspersky Digital Forensics and Incident Response operations are presented by Global Emergency Response Team (GERT), Computer Incidents Investigation Unit (CIIU), Global Research and Analysis Team (GReAT) with experts in Europe, Asia, South and North America, Middle East and Africa.

Verticals and Industries

Data in the report comes from our daily practices with organizations seeking assistance with full-blown incident response or complimentary expert activities for their internal incident response teams.
Noticeable impact on infrastructure such as encrypted asset, money loss, data leakage, suspicious e-mail led to 30% of requests for investigation. More than 50% of requests came from alerts in security toolstacks: endpoint (EPP, EDR), network (NTA) and other (FW, IDS/IPS, etc.).

Often organizations became aware of incident only after noticeable impact, even when basic security toolstacks had produced alerts uncovering some part of the attack. Lack of security operations staff is the most common reason to miss these indications. Suspicious files identified by security operations and suspicious endpoint activity led to uncovered incident in 75% of cases, while suspicious network activity in 60% of cases were false positives.

One of the most common reasons for an incident response service request is a ransomware attack: a challenge for detection even for mature security operations. For more details on types of ransomware and how to fight against this attack, visit our story "Cities under ransomware siege".

**Distribution of reasons for our top regions**

- Nature of biggest proportion – Suspicious file – shows file-oriented detection is still prevalent in a lot of organizations
- 100% of cases involving financial cybercrime and data leakages that we investigated appeared in CIS countries

**Distribution of reasons for selected industries**

- Surprisingly, 100% of money theft is inside the Financial industry (banks)
- Ransomware is detected after impact primarily within government, telecom and IT sectors
Initial vectors
Or how attackers got in

Dominant initial vectors are exploitation of vulnerabilities (0- and 1-day), malicious e-mails, and Bruteforce attacks. Patch management for 1-day vulnerabilities, applying password policies, and avoiding management interfaces on the Internet are well-suited to address most cases.

0-day vulnerabilities and social engineering attacks via e-mail are much harder to address and require a decent level of maturity from internal security operations.

Links between top initial compromise vectors and how the incident was detected

Sometimes we act as complimentary experts for primary incident response team from victim organization and we had no visibility into their findings – that’s why we have Unknown reasons on the charts.

Malicious e-mails are most likely to be detected by a variety of security toolstacks, but that's not showing distribution of 0- to 1-day vulnerabilities.

Distribution of how long the attack went unnoticed and how the organization was compromised

Our cases beginning with vulnerability exploitation on an organization’s network perimeter were the longest lasting.

Social engineering attacks through e-mail were the most short-lived.
Tools and exploits

30% of all incidents were tied to legitimate tools

In cyber-attacks, adversaries use legitimate tools which can't be detected as malicious utilities as they are often used in ordinary daily activities.

Suspicious events that blend with normal activity can be identified after deep analysis of malicious attack and connection of the use of these tools to the incident. The top used tools are PowerShell, PsExec, SoftPerfect Network Scanner, and ProcDump.

Most legitimate tools are used for harvesting credentials from memory, evading security mechanisms by unloading security solutions, and for discovery of services in the network. PowerShell can be used for virtually any task.

Let's weight those tools based on occurrence of such tool in the incident — we will also see tactics* where they are usually applied.

**Exploits**

Most of the identified exploits in incident cases appeared in 2019 along with well-known remote code execution vulnerability in Windows SMB service (MS17-010) being actively exploited by a large number of attackers.

**MS17-010**
SMB service in Microsoft Windows
Remote code execution vulnerability that was used in several large attacks such as WannaCry, NotPetya, WannaMine etc.

**CVE-2019-0604**
Microsoft Sharepoint
Remote code execution vulnerability allows attackers to execute arbitrary code without authentication in Microsoft Sharepoint.

**CVE-2019-19781**
Citrix Application Delivery Controller & Citrix Gateway
This vulnerability allows unauthenticated remote code execution on all hosts connected to Citrix infrastructure.

**CVE-2019-0708**
RDP service in Microsoft Windows
Remote code execution vulnerability (codename: BlueKeep) for a very widespread and unfortunately frequently publicly available RDP service.

**CVE-2018-7600**
Drupal
Remote code execution vulnerability also known as Drupalgeddon2. Widely used in installation of backdoors, web-miners and other malware on compromised web-servers.

**CVE-2019-11510**
Pulse Secure SSL VPN
Unauthenticated retrieval of VPN server user credentials. Instant access to victim organization through legitimate channel.

---

*MITRE ATT&CK*
### Attack duration

Kaspersky specialists have established the time period between the beginning of the attackers’ activity and the end of the attack. As a result of the subsequent analysis, all incidents were divided into three categories of attack duration.

<table>
<thead>
<tr>
<th>Rush</th>
<th>Average</th>
<th>Long lasting</th>
</tr>
</thead>
<tbody>
<tr>
<td>hours and days</td>
<td>weeks</td>
<td>months and longer</td>
</tr>
</tbody>
</table>

#### Common threat

- **Ransomware infection**
- **Financial theft**
- **Cyber espionage and theft of confidential data**

#### Common attack vector

- Downloading a malicious file by link in email
- Downloading a malicious file from infected site
- Exploitation of vulnerabilities on network perimeter
- Credentials guessing attack (bruteforce)
- Downloading a malicious file by link in email
- Exploitation of vulnerabilities on network perimeter
- Exploitation of vulnerabilities on network perimeter

#### Attack Duration (median)

- 1 day
- 10 days
- 122 days

#### Incident response duration

<table>
<thead>
<tr>
<th>Hours to days</th>
<th>Weeks</th>
<th>Months</th>
</tr>
</thead>
<tbody>
<tr>
<td>This category includes attacks lasting up to a week. These are mainly incidents involving ransomware attacks. Due to the high speed of development, effective counteraction to these attacks is possible only by preventive methods. In some cases, up to a week delay has been observed between the initial compromising and the beginning of the attacker’s activity.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This group includes attacks that have been developing for a week or several weeks. In most cases, this activity was aimed at the direct theft of money. Typically, the attackers achieved their goals within a week.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incidents that lasted more than a month were included in this group. This activity is almost always aimed at stealing sensitive data. Such attacks are characterized by interchanging active and passive phases. The total duration of active phases is on average close to the duration of attacks from the previous group.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Operational metrics

False positives rate
False positive for incident response is a very expensive activity. It means that triage of security event led to involvement of incident response experts who later identified that there is no incident. Usually this means the organization doesn’t have a specialist in threat hunting or they are managed by external SOC which doesn’t have context for the event.

Age of attack
This defines the time for incident detection by organization after the attack started. Usually detecting the attack in the early hours and even days is good. In case of more low-profile attacks it can take weeks which is ok, but taking months and years is definitely bad.

How fast we started
How long it took to start response after organization contacted us. In 70% of time we are working from day 1, but a variety of factors can influence the duration in some occasions.

How long response took
Distribution of time required for incident response activities.
Mapping to ATT&CK frameworks was done for about 50% of all incident response cases.

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Accounts</td>
<td>Windows Remote Management</td>
<td>Accessibility Features</td>
<td>Accessibility Features</td>
<td>Obfuscated Files or Information</td>
<td>Credential Dumping</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Service Execution</td>
<td>DLL Search Order Hijacking</td>
<td>DLL Search Order Hijacking</td>
<td>Masquerading</td>
<td>Network Sniffing</td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Windows Management Instrumentation</td>
<td>New Service</td>
<td>New Service</td>
<td>DLL Search Order Hijacking</td>
<td>Input Capture</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Scheduled Task</td>
<td>Scheduled Task</td>
<td>Scheduled Task</td>
<td>Software Packing</td>
<td>Credentials in Files</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Command-Line Interface</td>
<td>Registry Run Keys / Startup Folder</td>
<td>Process Injection</td>
<td>Process Injection</td>
<td>Account Manipulation</td>
</tr>
<tr>
<td>spear phishing Link</td>
<td>Graphical User Interface</td>
<td>Valid Accounts</td>
<td>Valid Accounts</td>
<td>Scripting</td>
<td>Brute Force</td>
</tr>
<tr>
<td>spear phishing Attachment</td>
<td>Scripting</td>
<td>Windows Management Instrumentation Event Subscription</td>
<td>Web Shell</td>
<td>Indicator Removal on Host</td>
<td>LLMNR/NBT-NS Poisoning and Relay</td>
</tr>
<tr>
<td>Third-party Software</td>
<td>Account Manipulation</td>
<td>Access Token Manipulation</td>
<td>Valid Accounts</td>
<td>Password Filter DLL</td>
<td></td>
</tr>
<tr>
<td>Rundll32</td>
<td>Web Shell</td>
<td>Hooking</td>
<td>Rundll32</td>
<td>Hooking</td>
<td></td>
</tr>
<tr>
<td>PowerShell</td>
<td>External Remote Services</td>
<td>Create Account</td>
<td>Connection Proxy</td>
<td>Web Service</td>
<td></td>
</tr>
<tr>
<td>Trusted Developer Utilities</td>
<td>Office Application Startup</td>
<td>Hidden Files and Directories</td>
<td>File Deletion</td>
<td>Modify Registry</td>
<td></td>
</tr>
<tr>
<td>Execution through Module Load</td>
<td>Hidden Files and Directories</td>
<td>Hooking</td>
<td>Code Signing</td>
<td>Trusted Developer Utilities</td>
<td></td>
</tr>
<tr>
<td>Mshta</td>
<td>Hooking</td>
<td>Access Token Manipulation</td>
<td>Deobfuscate / Decode Files or Information</td>
<td>Access Token Manipulation</td>
<td>Group Policy Modification</td>
</tr>
<tr>
<td>Component Object Model and Distributed COM</td>
<td>User Execution</td>
<td>Signed Binary Proxy Execution</td>
<td>Hidden Files and Directories</td>
<td>Mshta</td>
<td>Process Doppelgänging</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DCSHadow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Signed Binary Proxy Execution</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Group Policy Modification</td>
</tr>
<tr>
<td>Discovery</td>
<td>Lateral Movement</td>
<td>Collection</td>
<td>Exfiltration</td>
<td>Command and Control</td>
<td>Impact</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Application Window Discovery</td>
<td>Windows</td>
<td>Data from Network Shared Drive</td>
<td>Data Compressed</td>
<td>Data Obfuscation</td>
<td>Data Encrypted for Impact</td>
</tr>
<tr>
<td>Query Registry</td>
<td>Remote Management</td>
<td>Input Capture</td>
<td>Automated Exfiltration</td>
<td>Fallback Channels</td>
<td>Inhibit System Recovery</td>
</tr>
<tr>
<td>System Network Configuration</td>
<td>Third-party Software</td>
<td>Screen Capture</td>
<td>Data Encrypted</td>
<td>Custom Cryptographic Protocol</td>
<td>Stored Data Manipulation</td>
</tr>
<tr>
<td>Discovery</td>
<td>Pass the Hash</td>
<td></td>
<td></td>
<td>Standard Cryptographic Protocol</td>
<td>Runtime Data Manipulation</td>
</tr>
<tr>
<td>Remote System Discovery</td>
<td>Remote Desktop Protocol</td>
<td></td>
<td></td>
<td>Exfiltration Over Command and</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>Network Sniffing</td>
<td>Windows Admin Shares</td>
<td>Email Collection</td>
<td>Control Channel</td>
<td>Control Protocol</td>
<td>Resource Hijacking</td>
</tr>
<tr>
<td>Network Service Scanning</td>
<td>Replication Through</td>
<td>Data from Information Repositories</td>
<td>Exfiltration Over Physical Medium</td>
<td>Standard Application Layer</td>
<td></td>
</tr>
<tr>
<td>System Network Connections</td>
<td>Removable Media</td>
<td></td>
<td></td>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>Pass the Ticket</td>
<td></td>
<td></td>
<td>Multilayer Encryption</td>
<td></td>
</tr>
<tr>
<td>Process Discovery</td>
<td>Remote File Copy</td>
<td></td>
<td></td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Permission Groups Discovery</td>
<td>Component Object Model</td>
<td></td>
<td></td>
<td>Custom Command and Control</td>
<td></td>
</tr>
<tr>
<td>System Information Discovery</td>
<td>and Distributed COM</td>
<td></td>
<td></td>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>File and Directory Discovery</td>
<td>Exploitation of Remote</td>
<td></td>
<td></td>
<td>Standard Non-Application</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Services</td>
<td></td>
<td></td>
<td>Layer Protocol</td>
<td></td>
</tr>
<tr>
<td>Account Discovery</td>
<td></td>
<td></td>
<td></td>
<td>Web Service</td>
<td></td>
</tr>
<tr>
<td>Peripheral Device Discovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Share Discovery</td>
<td></td>
<td></td>
<td></td>
<td>Remote File Copy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Encoding</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Domain Fronting</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Remote Access Tools</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Domain Generation Algorithms</td>
<td></td>
</tr>
</tbody>
</table>