Ransomware
Case Study
Background

It seems ransomware is not only making a comeback, it’s here to stay. On 12 May 2017, an unprecedented global ransomware attack was launched, initially infecting over 230,000 computers in 150 countries. The attack has been described by Europol as unprecedented in scale, and has impacted organizations such as the UK National Health Service, Spain’s Telefónica and Germany’s Deutsche Bahn, while Russia has seen more infections than any other country with banks, the state-owned railways and a mobile phone network hit. The US delivery company FedEx was impacted, Nissan Motors’ UK manufacturing was halted, and Renault also stopped production in several sites in an attempt to stop the ransomware spreading further.

Previously McAfee had predicted ransomware will peak in the middle of 2017, and Kaspersky had labeled ransomware is the fastest growing security threat. Windows malware families such as WannaCry (the latest ransomware attack) Locky, Petya, or Samas, Mac OS X malware such as KeRanger, Linux (Linux.Encoder), and Android (Lockdroid), have been successful. The recent WannaCry ransomeware operation has shown a high level of dedication by its perpetrators, with the ransom demand message being localized into 28 different languages.

The motivation behind ransomware attack campaigns is to simply encrypt data on the infected host, and then demand payment in order to decrypt the data. The motivation is somehow similar to DDoS extortion attack campaigns (although much more “elegant” and harder to defend against), and puts the companies’ public servers in a denial of service condition, preventing them from serving legitimate clients, until the company is willing to pay the attacker. In the latest wave of the WannaCry ransomware, the impact was even more severe, with hospitals, health services and other mission-critical organizations such as banks, manufacturing and communications services being impacted.

This paper presents a real-life case in which empow’s security platform was able to detect, investigate and effectively mitigate a ransomware attack campaign at one of empow’s customer sites.

Main Attack Characteristics

Basic

In many ways the success of ransomware attack campaigns is a statistical one. This is because the basic attack tries to target hosts, for example through spear phishing, only some of which include important data that is valuable for the company or for the individuals clients who use the host (and who don’t have a backup for this data). The level of success of the attack campaign also depends on whether the users are tempted to download the malware, which isn’t always the case.

Advanced Campaigns

The more advanced types of ransomware campaigns address the statistical nature of the basic attack and make it more “effective”. These advanced campaigns use the following additional intrusions techniques:

- **Automatic internal propagation (“ransomworm”/ “cryptoworm”)**
  Once a host is infected, the malware scans for additional vulnerable hosts and propagates inside the network. This operation removes some of the human factor from the equation, as well as allows to reach hosts with more confidential data who are typically not accessible from the outside world.

- **Backup search and destroy**
  The malware automatically searches for backup files and deletes them, so there will be no way for recovery other than paying the ransom (or give up the data).
Challenges

The challenge to accurately detect and mitigate these threats lies in the fact that the ransomware campaign involves multiple stages, with each stage performing a malicious operation that might be flagged as suspicious (not a definitive high impact event) by a different security product, assuming the product is set with the right policy in place.

Processing each security event separately, with no layer of intelligence that can “see” the entire picture, analyze cause-and-effect relationships between the events, and make investigation and pro-active prevention decisions in real-time, results in one of the following negative results:

Mis detection
Each alert looks suspicious but not risky enough to set off preventive operations, so the attack goes on successfully and infects the hosts in the organization.

False Positives
Trying to execute intrusive prevention measures upon identification of each suspicious event results in an excessive amount of false positive decisions that leads to blocking of legitimate users in the organization.

Delayed Response
Collecting the excessive amount of events generated by today’s security solutions, and investigating them by the analysts in the SOC is a time consuming operation that results in a delayed response to the attack.
**Attack Steps**

The following section illustrates the typical operation of the ransomware attack campaign and the capabilities of the various security technologies to detect the different stages of the attack. It will shed more light on the detection and prevention challenges:

![Ransomware attack campaign diagram](image)

**Stage 1**
**Spear Phishing**

A stage that typically will not be detected by any security tool and can be considered as the social engineering stage that tries to lead some of the users to open the mail and click on a link.

**Stage 2-3**
**Malware Download**

A stage in which the user tempted to click a link that leads him to download a malware from a website. A threat intelligence service feed can flag on it with an alert about access to a potentially bad reputation URL. Reputation alerts are not considered accurate indications of compromise (IOC) and therefore will typically not be followed by any preventative measures.

**Stage 4**
**Sandbox Alert**

At this stage the network based anti-malware (sandbox device) copies and executes the downloaded file object, and generates an alert about a zero-day malware*. This sandbox alert doesn’t imply any impact and because of this will typically create a task for a security engineer in the IT team to go and investigate the host (while the host is already infected).

---

* It is pretty easy to create new malware revisions through malware kits, which will cause sandbox technologies to identify them as zero-day malware without a definitive decision about the type and the malware’s impact.
Stage 5
C2 Communication

At this stage the infected host accesses a command and control server in order to receive the encryption key or to share the key it used for the encryption (depends on the malware type). The threat intelligence service can flag this activity (e.g. possible communication with a C2 site, however it will not automatically associate it with the sandbox event and the previous access to the bad reputation URL that took place already). The alert will not be considered a definitive and accurate IOC and therefore will not be followed by any prevention measure. The same basic attack campaign scenario continues to target each one of the organization’s clients in the same way, attempting to infect more clients as much as possible – all without any response that can prevent it in time.

![Figure 2. Advanced ransomware campaign.](image)

Stage 6
Malware Scan

At this stage the malware scans the network to find vulnerable hosts. The scan activity is detected by the NBA (Network Behavior Analysis) security solution, however because the event is not automatically associated with previous events of the same host, it will be considered a low risk one (if it is noticed at all among all the other events), and hence no blocking will be executed to prevent further such activities from fear of false positives.

Stage 7
Malware Propagation

Upon identification of vulnerable hosts, the malware will aim to infect them through a few optional methods such as remote desktop servers that are compromised, vulnerable file sharing services etc. This activity can be flagged as an abnormal network activity by NBA security solution (in case it inspects internal organization traffic). However, as in the previous case, it will be considered a low risk event with no definitive risk and impact and therefore no blocking decision will be made. It should be noted that network-based anti-malware solutions (sandboxes)* don’t typically process east-west traffic (mainly for performance and deployment complexity issues, only north/south traffic is analyzed), therefore the anti-malware solution will not analyze the traffic that includes propagation attempts.

* A host based sandbox might exist, but again it will typically identify a suspicious activity with no definitive impact.
Protecting Against Ransomware Campaigns

empow’s security platform integrates with your existing network infrastructure, and then breaks your security tools down to their individual components, what we call “security particles”.

This creates an abstracted new layer that sits above your existing security configuration, and **turns what you have into what you need.**

When the platform identifies an event, a new, targeted apparatus is instantly reassembled and deployed for each individual attack. This automates detection, investigation and the mitigation actions in your network - in real time. This means quicker and smarter responses, with better correlation and insight.

The high level architecture of our platform is shown below. For more information about the technology, architecture and how security apps are defined, please refer to the Technology White Paper.

---

**Figure 3.** The architecture
This use case presents how the anti-ransomware security app adaptively orchestrates security resources in the network in order to detect, investigate and proactively mitigate the attack campaign in real-time. The empower Ransomware Security App orchestration model includes the following security services and functions:

**Detection Phase**

The following security services and functions (what we call “security particles”) were configured in the detection phase of the security app in order to collect and correlate their security events:

- **Reputation service** with 3 security functions: phishing, C&C and malicious URLs.
- **NBA service** 3 security functions: New Flow Anomaly (NFA), Anti-Scan, Probe & Malicious Cmd.
- **Anti-Malware service** with 2 security functions: Ransomware and Zero-day.

**Investigation Phase**

The following security services and functions were configured in the investigation phase in order to create and enforce investigation policies on hosts that were discovered as suspicious in the detection phase:

- **Anti-malware service** with 3 security functions: Ransomware, Spyware and Zero-day.

**Mitigation Phase**

The mitigation phase was configured with a **mitigation service** that includes application filters security function. Once the system identifies a high risk ransomware attack campaign activity, it will automatically activate the mitigation service and will configure it with a pro-active mitigation policy that prevents the attack.

---

**Figure 4. Ransomware security app (Orchestration model).**
Detection, Investigation & Mitigation by the Security Platform

The security app defined above, orchestrated multiple security services in order to come to a fast and accurate conclusion about a high impact ransomware attack campaign that is developing against users in the organization. With reference to Figure 1 (Basic ransomware operation), this section describes the security app operation that leads to pro-active mitigation of the threat:

Security App Detection Phase Operation

1st Client Infection Attempt

With reference to the figure below (Risk-chain dashboard):

- The security app collects events from the reputation service. The malicious URL function (defined as engine in the popup below) identified the event as "reputation malicious URL". This event identifies that a client (blue point) is trying to access a bad reputation URL (red point).

- As shown on the segment (green line) popup and in the segment risk-chain table, the event is automatically classified as threat type "Propagation" and the associated segment risk is set Low (L) while the overall attack risk is set info (i).

Risk-chain dashboard

Risk-chain table
The security app continues to collect events from the reputation service. The C2 function (engine) identified the event: "Reputation C&C". This event identifies that the client established a communication with a suspicious command and control site and therefore classified as C2 threat type (shown as a second segment from the same client to another bad reputation site).

The risk-chain discovery module (empow's security analytics engine) automatically identifies cause-and-effect relationships between the security events, i.e., a command and control event followed by access to a bad reputation URL event from the same client. The fact that cause and effect was identified for this client is indicated in the effect field in the host popup (as shown below). It should be noted that the cause-and-effect identification conducted by the Security Platform CyberCreate doesn’t require security analysts to define or maintain correlation rules (an intensive resource-consuming task that typifies SIEM systems).

Because of the C&E relationships, the associated segment risk is set high (H) while the overall attack risk is set low (L).
Security app investigation phase operation

- At this stage, the security app decides to investigate the client (investigated host symbol: 🌐). Investigation is executed by the anti-malware functions, which are automatically assigned according to the suspicious activity detected on the client.

- As shown in the pop-up, the spyware, zero-day, spyware and ransomware anti-malware root-cause investigation functions were activated, searching for past events that can indicate download of a malicious file.

![Investigation Functions](image)

- As shown in the event details table below, the zero-day malware function (engine) identified a security event. The event indicates that the file which the client tried to download was executed in a sandbox environment (by the LastLine product) and suspicious activities were identified with no indication regarding to which malware type is it.

### Events details table

<table>
<thead>
<tr>
<th>Time</th>
<th>Phase</th>
<th>Service Name</th>
<th>EE Name</th>
<th>Event &amp; Count</th>
<th>Source</th>
<th>Destination</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>22:05:16</td>
<td>DETECTION</td>
<td>Reputation Service</td>
<td>Malicious URLs</td>
<td>(D) Reputation Malicious...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22:05:16</td>
<td>INVESTIGATION</td>
<td>Anti-Malware Service</td>
<td>Zero-day</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Investigation phase zero-day event](image)

- Drilling down from the event details table to vendor attack details table, shows the attack description as defined by the vendor (LastLine).

![This threat indicates that a malicious executable (malware) was downloaded by a protected host. The host that downloaded the file has likely been infected by the downloaded malware, unless an Anti-Virus product installed on the host was able to detect and mitigate the threat.](image)
The risk-chain discovery module automatically identifies a 2nd cause-and-effect relationship, i.e., a command & control event followed by access to a bad reputation URL event – both from the 2nd client. Because the number of attack segments and cause-and-effect relationships were increased for the overall attack, the attack risk level was automatically set high (H) as shown in the risk-chain table below.

Because the attack risk reached a high level, the security app executed the operation of the mitigation phase.

With reference to the figure below:

- The same attack activities are identified against a 2nd client in the organization.
- Because the risk-chain discovery module analyzes that the same bad URL site and C2 site are used, it automatically groups the new security events with the same existing attack (of the 1st client) and thus exposes it to be one attack campaign as shown below.

- As in the case of the 1st client, the security app activated the investigation functions which identify zero-day malware download.

Risk Chain Discovery Cause-and-Effect Analysis

Risk Management

- The risk-chain discovery module automatically identifies a 2nd cause-and-effect relationship, i.e., a command & control event followed by access to a bad reputation URL event – both from the 2nd client. Because the number of attack segments and cause-and-effect relationships were increased for the overall attack, the attack risk level was automatically set high (H) as shown in the risk-chain table below.

- Because the attack risk reached a high level, the security app executed the operation of the mitigation phase.
The risk chain discovery layer analyzes the established attack pattern in order to create mitigation rules. The following pattern is analyzed:

- The same bad URL sites and C2 sites are accessed by two clients in the organization in a suspicious sequence, i.e., a sequence that shows a cause-and-effect relationship.
- Both suspicious clients were identified as hosts that are attempting to download a zero-day malware from the same site.
- Below illustration shows the similarity that the system identifies:

Based on the risk-chain pattern, the system identifies that multiple clients are the target of the same attack scenario – an attack campaign.

The mitigation phase generates a proactive mitigation rule and executes it in the relevant firewalls in the network (as shown in the illustration below):

![Diagram of security app mitigation phase](image-url)
The system generates an ANY-> Bad reputation site drop rule, which allows to proactively block any further attempt to infect clients by the ransomware attack campaign.

The drop rules that the system executes are specified in the mitigation table:

The blocked hosts are highlighted in orange in the attack risk chain dashboard:

As can be seen a new client (a 3rd one at the upper right area), that tried to access the same bad reputation site, was blocked by the proactive drop rule. Thus, the ransomware security app was able to prevent any further infection attempts.
The Value

The above attack prevention use case shows how empow’s ransomware security app created a solution that orchestrates multiple security resources in order to automatically identify an attack campaign pattern and execute proactive mitigation rules.

Given the statistical nature of the ransomware attack campaign, the Ransomware security app provides an effective mitigation of both basic and advanced ransomware attack campaigns.

This use case highlights the following main values of the Security Platform:

**Effective Security**

Effective security is achieved through an orchestration of multiple security products, which couldn’t be achieved by each product separately. As mentioned in the background section, alerts raised by each individual product are not definitive enough for the decision making.

**Automation**

Automation and reduction of many of the tasks that need to be done by security analysts and network security engineers, including:

- Creation and execution of the most effective detection and investigation policies.
- Searching and analyzing cause-and-effect correlations among millions of security events.
- Creation and maintenance of static correlation rules in SIEM systems.
- Identifying attack risk chain patterns and managing risk accordingly.
- Generating predictive mitigation rules.

Given the fact that most of the operations that the security platform executed need to be done by humans (when empow’s security platform is not in place), it was proven that empow’s platform reduced the overall time to detect, investigate and mitigate the attack from weeks to minutes, while preserving the IT security expert resources to deal with other security challenges.