



# **Anatomy Of A Targeted Ransomware Attack**

## A True Story Of A Recent Incident Response To An Industrial Ransomware Cyber Attack

January 2020

White Paper

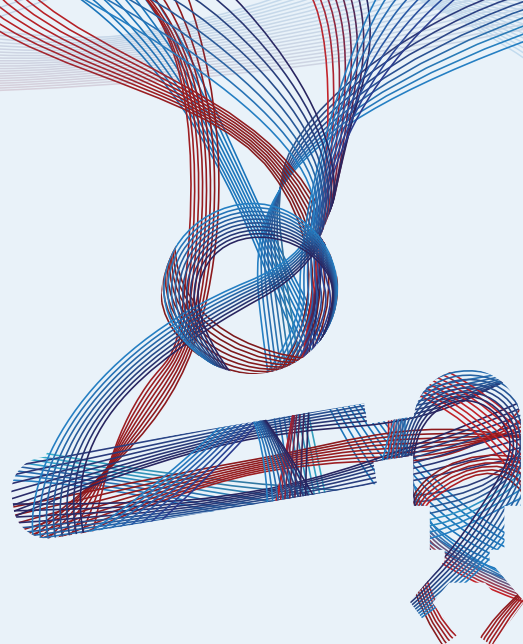
By: Ofer Shaked, Co-Founder & Chief  
Technology Officer

## Table of Content

|                                                       |    |
|-------------------------------------------------------|----|
| Overview                                              | 01 |
| The Ransom Note                                       | 02 |
| Incident Response Team Is Called On-Site              | 03 |
| Gathering the Evidence                                | 04 |
| Here is Where the Team Started Looking                | 05 |
| The Evidence Analysis                                 | 06 |
| The Initial Findings                                  | 07 |
| Caught Red Handed                                     | 08 |
| Closing the Loop                                      | 09 |
| Additional Attack Methods Used by the Cyber Attackers | 10 |
| Further Analysis                                      | 11 |
| Conclusions and Next Steps                            | 12 |
| Don't Be Scared, Be Prepared                          | 14 |
| Message from the Author                               | 15 |

# Overview

---



*SCADAfence's Incident Response team assists companies in industrial cyber security emergencies. In this whitepaper, we will review a recent incident response activity in which we took part.*

*This whitepaper has been published with the goal of assisting organizations to plan for such events and reduce the impact of cyber-criminals on their networks.*

*The company that was attacked didn't have the SCADAfence Platform deployed at the time of the attack. The SCADAfence Platform was installed upon the arrival of our Incident Response team as part of the investigation, and helped them to contain the threat.*

*The SCADAfence Incident Response team was assisted by the SCADAfence Reverse Engineering team and by the SCADAfence Research teams, in order to gain knowledge on the cyber attackers and to contain the attack.*

# The Ransom Note



Late at night on November 24th, critical services suddenly stopped working at the largest manufacturing facility of Umbrella, Inc.\*, an international pharmaceutical company. An investigation was immediately launched. While investigating the issue, the local IT team found ransom notes on a number of devices in the network, requesting the company to contact a certain email address and to make a payment in Bitcoin.

The IT team immediately called Mr. Birkin\*, the Group IT Leader who was sleeping soundly. He immediately woke up and rushed to the plant, while more and more devices started showing the ransom note.

During the 7 hours of the attack, around 200 critical servers were encrypted, and the entire production network was down as a result.

The company evaluated the situation and came to the conclusion that they would pay the ransom in Bitcoin. But then the attackers decided to change their price, which made the company completely lose their trust in the cyber criminals, and they decided not to pay the ransom to the cyber criminals.

# Incident Response Team Is Called On-Site

SCADAfence's Incident Response (IR) team was then urgently called to the site, which is located in a relatively remote industrial area. On the way to the site, the SCADAfence IR team was briefed on the situation, and then provided initial containment instructions to the on-site security team.



## Initial Response Instructions

**The goals of the initial instructions, before the SCADAfence IR team arrived on-site, were as follows:**

1. Contain the threat to a specific area of the network and prevent infection of additional networks.
2. Eliminate or minimize downtime of unaffected systems, without exposing them to additional risks.
3. Keep evidence in an uncontaminated state. Contaminated evidence hampers an investigation.



## Incident Response Goals

**The SCADAfence IR team arrived at the site and received the following objectives from Mr. Birkin:**

1. Identify the initial attack vector (how the attackers got into the network in the first place).
2. Understand the propagation methods.
3. Identify all of the machines that are infected.
4. Monitor for any additional suspicious activity to make sure there are no backdoors through which the cyber attackers could gain re-entry.

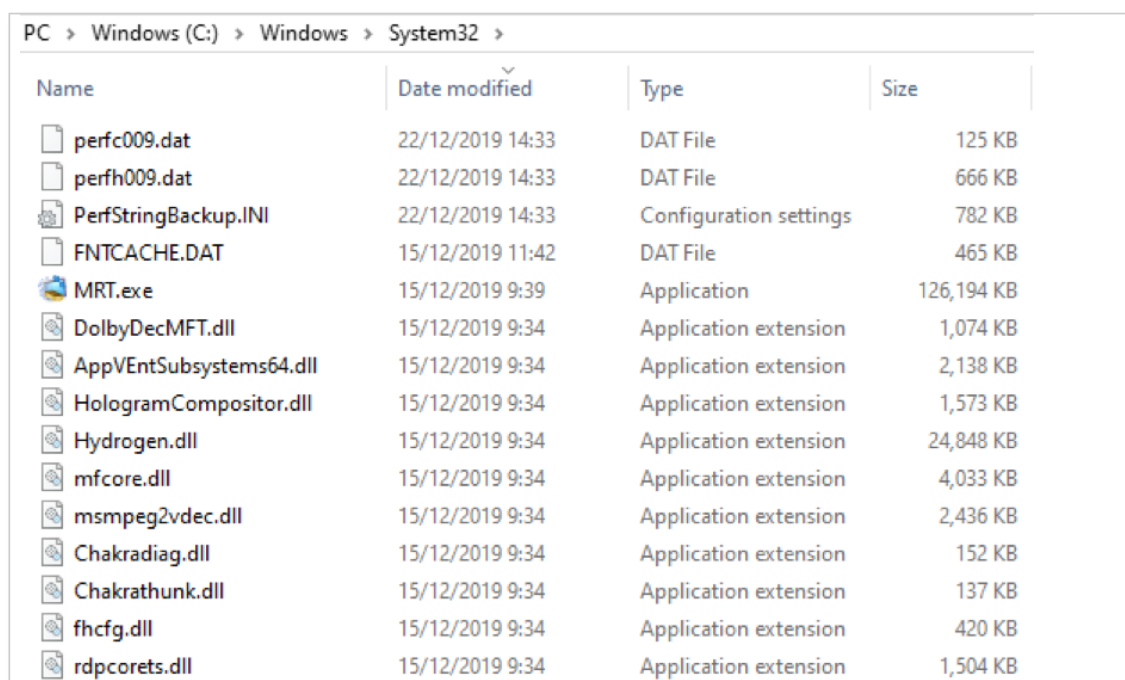
The IR team was then briefed by the site's engineers and managers about the situation, and they decided together on the next steps to achieve those goals.

# Gathering the Evidence

After the IR team understood the entire situation, the first step they took was to gather the evidence as soon as possible. The evidence included images of the systems, the log files, the configuration files, and basically anything that might contain information which could be important for the investigation.

The reason for the urgency is because many sources of evidence are cyclical, meaning they are

automatically deleted after a while by fresh new data. Some evidence is saved without historical data (such as file timestamps), and can become contaminated with new information if the team waits for too long. The attackers can attempt to delete evidence (such as exploits, malware files), and sometimes people who are trying to be helpful but aren't experienced in cyber security can also contaminate or delete evidence accidentally.



| PC > Windows (C:) > Windows > System32 > |                  |                        |            |
|------------------------------------------|------------------|------------------------|------------|
| Name                                     | Date modified    | Type                   | Size       |
| perfc009.dat                             | 22/12/2019 14:33 | DAT File               | 125 KB     |
| perfh009.dat                             | 22/12/2019 14:33 | DAT File               | 666 KB     |
| PerfStringBackup.INI                     | 22/12/2019 14:33 | Configuration settings | 782 KB     |
| FNTCACHE.DAT                             | 15/12/2019 11:42 | DAT File               | 465 KB     |
| MRT.exe                                  | 15/12/2019 9:39  | Application            | 126,194 KB |
| DolbyDecMFT.dll                          | 15/12/2019 9:34  | Application extension  | 1,074 KB   |
| AppVEntSubsystems64.dll                  | 15/12/2019 9:34  | Application extension  | 2,138 KB   |
| HologramCompositor.dll                   | 15/12/2019 9:34  | Application extension  | 1,573 KB   |
| Hydrogen.dll                             | 15/12/2019 9:34  | Application extension  | 24,848 KB  |
| mfccore.dll                              | 15/12/2019 9:34  | Application extension  | 4,033 KB   |
| msmpeg2vdec.dll                          | 15/12/2019 9:34  | Application extension  | 2,436 KB   |
| Chakradiag.dll                           | 15/12/2019 9:34  | Application extension  | 152 KB     |
| Chakrathunk.dll                          | 15/12/2019 9:34  | Application extension  | 137 KB     |
| fhcfg.dll                                | 15/12/2019 9:34  | Application extension  | 420 KB     |
| rdpcorets.dll                            | 15/12/2019 9:34  | Application extension  | 1,504 KB   |

*File modification dates are easily contaminated with fresh data, if not investigated immediately*

If not investigated immediately, file modification dates can easily be contaminated with fresh data. The SCADAfence IR team found out that, unfortunately, due to a lack of synchronization between the company's IT team prior to their arrival on the site some of the evidence had been contaminated or lost. For example, some machines

had been restored from backups without prior imaging and some logs had been lost because they weren't saved in time (prior to the automated deletion cycle).

Ideally, the IR team should run forensics on all the machines; but in order to save time, the team needed to make educated guesses on where to start.

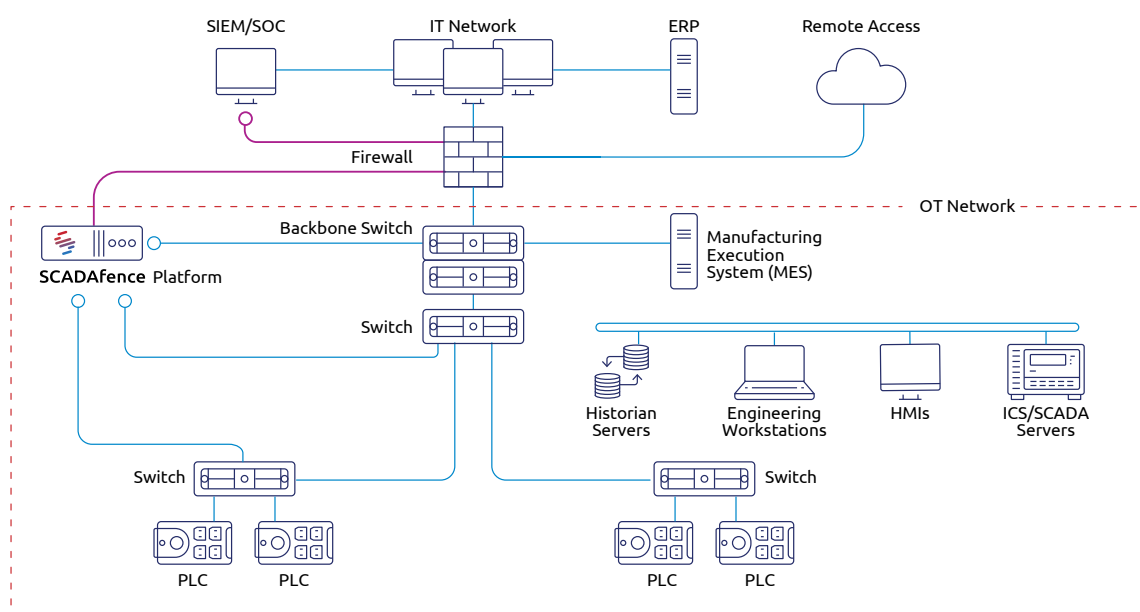
# Here is Where the Team Started Looking:

- 1** Machines that showed signs of infection before others.
- 2** Machines that were central in many attacks, such as domain controllers.
- 3** Machines that showed signs of malicious activity in addition to the ransomware operation – for example machines that have other attack tools on them. Such information can be gathered from alerts in the already-installed security mechanisms.
- 4** Other machines that are suspicious for other reasons.

While on the way, the IR team requested that the company's IT team should create images of all the infected machines, and if impossible (such as in the case of embedded devices like PLCs/switches, etc), they should at least gather all of the logs from the devices. This process should be performed by someone who is familiar with the type of evidence that each type of device can offer and who is able to find the logs that are relevant from a cyber-security

point of view.

On-site, the SCADAfence Platform was installed on the backbone switch in order to later assist in detecting and documenting any suspicious activity going forward. The SCADAfence IR team knew that the attackers would still have access to the network and the team wanted to see what the attackers were doing in the network, and also to recognize any more infected machines and/or possible access vectors.



*The SCADAfence Platform installed on the backbone switch*

# The Evidence Analysis



The images have been analyzed by the SCADAfence forensics team. The SCADAfence forensics team inspected the configuration of the machines, the suspicious executables, the log files, the file timestamps, the event logs, the suspicious files and everything else that could be relevant. All of the suspicious executables and binary files were sent to the SCADAfence Reverse Engineering (RE) team for further analysis.

The SCADAfence RE team is capable of quickly understanding any type of attack method and tools, and has the ability to find IOCs (Indicators of Compromise) in binaries and executables, such as C&C (Command & Control) server addresses, passwords, and other similar valuable information.

”

*The SCADAfence Reverse Engineering team is capable of quickly understanding any attack method and attack tools.*

*They also have the abilities to find Indicators of Compromise in binaries and executables.*

# The Initial Findings

Several minutes after sending the executable files to the SCADAfence Reverse Engineering team, it was discovered that the attackers used a unique malware sample without any shared IOCs with other malware, which had prevented it from being detected by signature-based methods.

The team also found the IP addresses of the new C&C (Command & Control) servers, together with the multiple connection methods they support.

This allowed the SCADAfence IR team to go to the organizational firewall, filter for those IP addresses and ports, and get a list of all the infected machines.

The full list included infected machines that the IT team had not been aware were infected. As a result of this effort, they started reinstalling or restoring those machines from backup immediately. Infected machines can reinfect other machines, so it is critical to work on them as soon as possible.



# Caught Red Handed



A few hours after investigation started, the newly installed SCADAfence Platform reported a network scanning activity from one of the machines which was not on its list of infected machines. This machine was a server, central to the operation of the network and had multiple network interfaces (NICs) plus special firewall rules that allowed it to communicate with other network segments. The SCADAfence Platform reported that this server was scanning segments that were not infected, over ports 445 TCP (SMB) and 3389 TCP (RDP). The scanning activity was not visible in the firewall logs because some of the networks had been bridged using NICs installed on the machine rather than by being routed through the firewall.

The customer was unaware of such configurations, and assumed that all cross-segment traffic was routed through the firewall.

As a result of the scanning event, the SCADAfence IR team understood that the attackers were looking for additional segments to infect, and they decided to shut down all machines that have multiple NICs, as at least one NIC had been shared with the infected segment. This was a high price for the customer to pay, but it was the SCADAfence IR team's recommendation because it was the only way to limit the attack surface. On this newly infected machine, additional attack tools were discovered, such as the network scanner that was used by the attackers.

# Closing the Loop

This machine was managed by an external contractor for the purpose of maintenance and support. It had an external IP address, which prevented the IR team from finding it in the firewall logs (these were filtered on connections from inside to the outside). It had internet connectivity open to only one IP – the IP of a machine that was managed by the external contractor. The machine's event log showed an RDP connection from the external machine approximately 1 hour before the attack had begun. With the guidance of the vendor, the SCADAfence IR team connected to the external machine and reviewed its logs:

**Here is what they discovered:**

- 1** It had an RDP port open to the internet.
- 2** It was unpatched.
- 3** It had no endpoint protection software.
- 4** Windows Defender was disabled.
- 5** It had a "twin" log event of connecting to the internal machine at the same time.

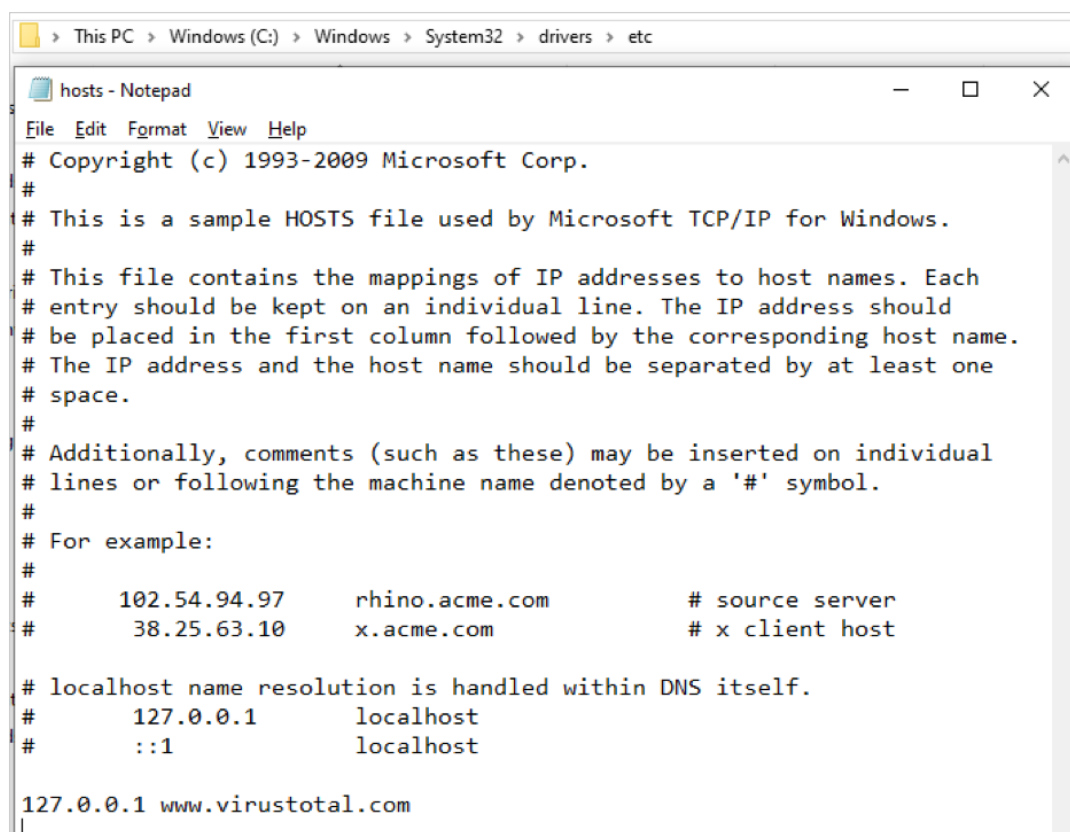
”

*These pieces of evidence confirmed that the origin of the attack was the external server, which had been left unpatched and was exposed to the internet and maintained by a vendor with little awareness of cyber security. The entire investigation took the SCADAfence IR team about 10 hours.*

# Additional Attack Methods Used by the Cyber Attackers

In addition to the main attack methods, which were an RDP vulnerability, a C&C server and a ransomware executable, the cyber attackers also used additional attack methods that were discovered in the SCADAfence Platform such as:

1. Patching the hosts file to prevent access to the VirusTotal malware analysis service.
2. Disabling Windows updates.
3. Hiding executables in legitimate folders.
4. Locking any input devices during the encryption process.
5. Disabling the endpoint protection software.
6. Using Mimikatz to successfully extract and use Domain Admin Kerberos tickets.



```
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com             # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost

127.0.0.1 www.virustotal.com
```

*A patched hosts file (C:\windows\system32\drivers\etc\hosts) showing how VirusTotal traffic is redirected to localhost.*

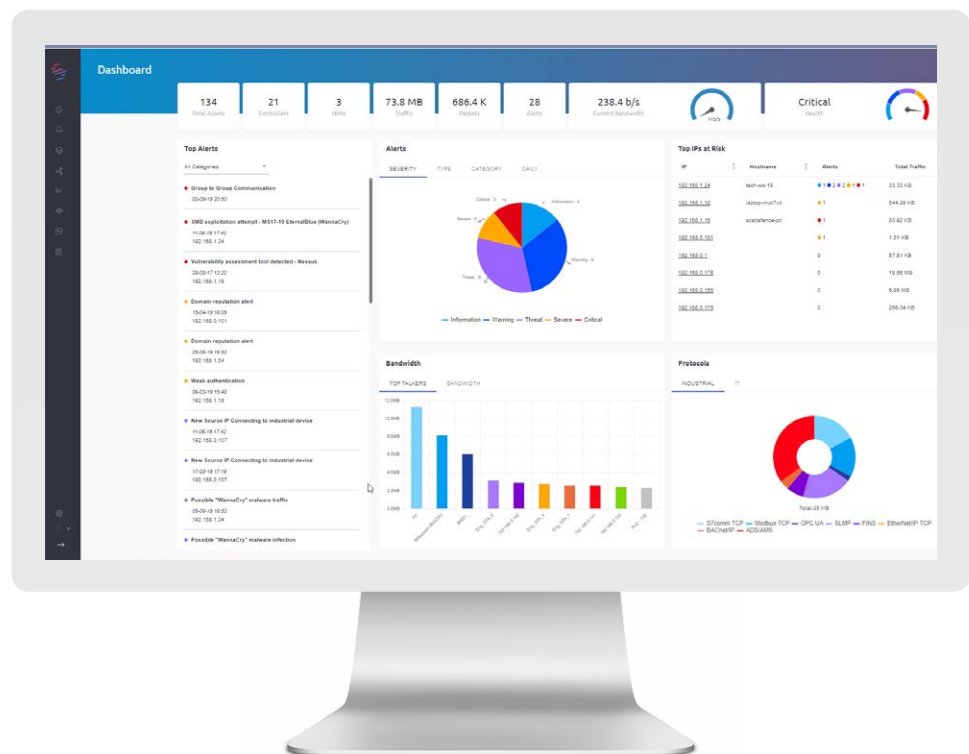
# Further Analysis

The attackers may have generated additional backdoors into the network, so continuing monitoring with the SCADAfence Platform is crucial to ensure that the whole network does not become reinfected.

**In addition to that, the SCADAfence Platform has:**

- 1** Detected multiple, high-risk policy violations, after configuring the company's security policy in the SCADAfence Governance portal.
- 2** Mapped all external to internal and internal to external access points.
- 3** Mapped the connectivity between network segments, including legacy and hidden connections that were unknown to the customer.
- 4** Detected additional wormable vulnerabilities in both the industrial and IT equipment, that should be patched or contained.
- 5** Detected additional security events over the course of the weeks following the attack.

These findings allowed the IT team to prevent similar future attacks from happening again, thereby reducing risk exposure.



# Conclusions and Next Steps

The SCADAFence Research team has compiled a list of steps that could have prevented the cyber-attack or could have seriously limited the attack's impact:

1. A network monitoring system with a firewall integration, like the SCADAFence Platform, could have prevented the attack. When cyber attackers are scanning the network, the network monitoring system could have automatically isolated the device, disconnecting it from the internet and sending it to the IT team for further review. This would have ended the incident before the machine started infecting any other machines.
2. A proactive approach would have been much more cost-effective to execute, as opposed to being attacked and handling the cyber-attack incident later on. The proactive approach allows security teams to know in advance if they have any policy violations, or if they have any network or device vulnerabilities, and they can perform prioritization. A machine that is open to the internet, and is also a part of a large subnet with critical servers, is easy to detect and would have been prioritized as a critical finding by a network monitoring platform such as the SCADAFence Platform.
3. Have off-site backups of important systems and test restoration procedures from time to time. Have at least 1-2 older backup points, for example from 90 and 180 days ago (if your storage allows it). Otherwise, the IT teams might be restoring a backup from last week that's still infected with malware. Restoring from an infected backup can severely prolong the restoration time.
4. The SCADAFence IR team reviewed all of the Domain Admin accounts along with the customer and helped them change all of their passwords. The IR team also reviewed all Kerberos related configurations and reset the KRBTGT password.



*A network monitoring system with a firewall integration, like the SCADAFence Platform, could have prevented the attack*

5. Kerberos tickets must timeout as recommended by Microsoft – 600 minutes or less.
6. All externally facing services should be micro-segmented. Access to, and from them should be restricted.
7. A secure remote connectivity solution must be put in place, such a solution is available by using SCADAfence and CyberArk.
8. All remote connections should include 2-factor authentication.
9. Network segments must be put in place in a way that traffic between them is limited to specific services only, and not “any -> any” rules. They should be defined in a way in which an infection of an entire segment won’t halt the operation of the entire network. Therefore, it’s not recommended to use one segment for all of the critical servers. Some servers, such as Domain Controllers, should have their own segment.
10. All machines that require internet connectivity should be configured to use a central server in the DMZ instead of talking directly to IP addresses.
11. Machines that are required to browse the internet (host->any rule), should not be able to directly communicate with industrial devices or vulnerable devices.
12. Start a software vulnerability management process (if you don’t already have one).



*A proactive approach would have been much more cost-effective to execute, as opposed to getting attacked and later handling the cyber-attack*

# Don't Be Scared, Be Prepared

This organization did not wait for a cyber-attack to start their cyber security program. They were in touch with other security companies prior to the attack. However, they weren't fast enough and the vulnerabilities were critical enough for attackers to gain access into the network and to cause damage.

## **A well-prepared network is:**

- 1. Very difficult to attack.**
- 2. Slows down the attackers, and allows the defenders to take action.**
- 3. Still attacked occasionally, but the damage caused is minimal.**

For example, in this specific network there were around 5,000 devices, but only 200 servers were attacked. The reason for this is a network segmentation solution that they had in place. Otherwise, they would now be recovering from a 5,000 devices ransomware attack.





### *Message from the author:*

If you find value in the findings in this report and would like a 1-hour security review of your industrial network, I would be happy to help.

It will be a free consultation, with me, and with no strings attached - all under NDA.

I will give you my recommendations based on your specific security needs – after seeing hundreds of industrial networks and I will help you remediate any security issues that you might have in your network.

Yours truly,  
**Ofer Shaked**

CTO & Co-Founder of SCADAfence  
Over a Decade in OT Security  
Security Architect in the OT Cyber Security Alliance (OTCSA)  
On the ManuSec Advisory Board  
Keynote Speaker at SANS events

Dates, names and other minor details have been changed or deleted in order to anonymize the report.

## About SCADAFence

SCADAFence is the global technology leader in OT cyber security. The solution enables organizations with large-scale OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and user experience. The SCADAFence solution seamlessly integrates OT security within existing security operations, bridging the IT/OT convergence gap. SCADAFence delivers security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAFence enables organizations in manufacturing, building management and in critical infrastructure industries to operate securely, reliably and efficiently as they go through the digital transformation journey. To learn more go to [www.scadafence.com](https://www.scadafence.com)

### Our offices

Headquarters: Tel Aviv

Regional: New York, Munich, Tokyo

Contact us: [info@scadafence.com](mailto:info@scadafence.com)

[www.scadafence.com](https://www.scadafence.com)



**SCADAFence**