2017. 07. 12

Tech Report

# Targeted Attacks on Defense Industry

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | www.AhnLab.com | 

# Table of Contents

# Introduction

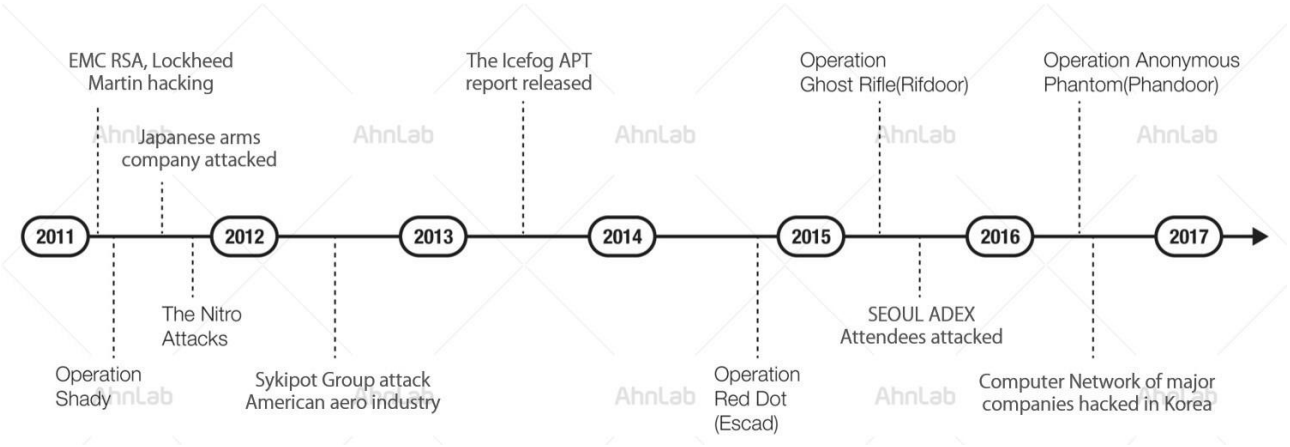
Cyberattacks on the defense industry were first discovered in 2010 and has been consistently intensifying. The defense industry is comprised of companies that manufacture defense logistics and is highly likely to be the target of attacks from hostile countries or competing countries due to the magnitude of control once security is breached.

Recently, a defense industry has again been a target of attack and even reported cases of attack in the political and diplomatic sector. It is presumed that the attackers not only sought trade-secrets in the defense industry, but also sensitive information related to national security.

This report, based on case studies, outlines the recent trends of cyberattacks on the defense industry.

# Finding 1: Timeline of Main Attacks on the Defense Industry

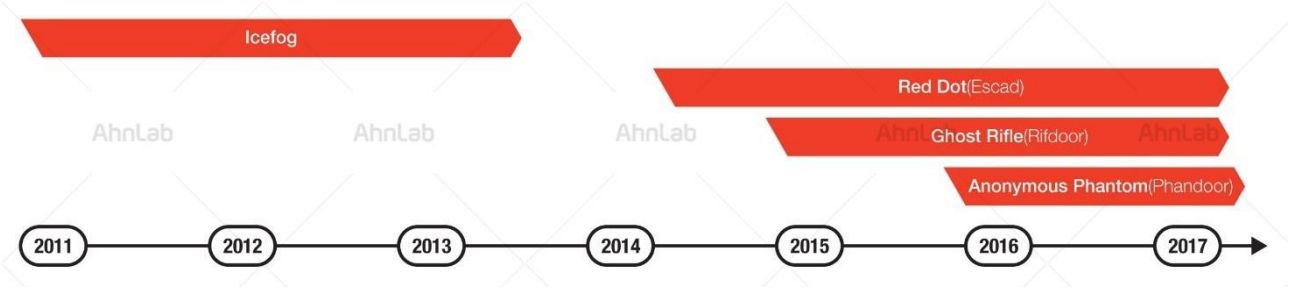
The primary attacks on the defense industry reported by the defense company or the media are shown in *Figure 1*. Illegal activities of at least four hacking groups have been monitored since 2010.




[Figure 1] Timeline of main attacks on the defense industry

The timeline of activity by the main hacking groups which attacked the defense industry can be found in *Figure 2*.




[Figure 2] Timeline of activity by the main hacking groups

*Icefog*, one of notable hacking groups, has been active from sometime in 2011 up to October 2013. However, there is a possibility that they are currently using a different malware although that has yet to be confirmed. *Red Dot* was active from June 2014 to the end of 2016, and used a malware named *Escad*. However, a malware that might be the initial version of Escad was found earlier in 2013. This group is also considered to be behind the attack on the Sony Pictures Entertainment in November 2011. In 2016, they began to attack defense industry and other companies.

*Ghost Rifle* emerged in 2015 and mainly uses malware named *Rifdoor* and *Ghostrat*. *Ghost Rifle* collaborated with *Red Dot* to attack companies who participated in South Korean defense industry conference, 2015. In addition, this group is linked to an attack on security companies and major companies in early 2016. *Anonymous Phantom* emerged in early 2016, but has since become less active. However, they were found to have been behind the attack on an energy research center this spring.

*Escad*, used by *Red Dot* is found in C&C servers around the world. Moreover, the C&C servers of *Rifdoor*, found between 2015 and 2016 and *Phandoor,* which came right after *Rifdoor*, were found to be using local university systems.

# Findings 2: Methods of attacks

The analysis of the attacks made on the defense industry around the world indicate that attack methods in defense industry can be divided into three; email, watering hole and central management system. Most attacks were found to have targeted the central management system.

## 1. Email

Attackers usually glean information of their victim first to design a specific email which will entice the victim to open the attachments or link. The content of the email is usually related to the victim's area of work or on global issues. In general, .docx, .xls, or .pdf files were embedded with malware and activate once the user opens the file. Sometimes execution files, such as .exe or .lnk files were disguised as document files.

## 2. Watering hole

For the watering hole attack, a specific group is targeted. An attacker first guesses or observes which website is frequently visited by their target. The attacker will then attack the website to hide a malware which will infect the victim's system when they access the compromised site via vulnerable web browsers. In some cases, attackers may only infect users with specific IP address, making it harder to detect.

## 3. Management System

The hacking of the cybersecurity companies and major companies in 2016 used an attack method to attack the central management system to distribute malware on all connected computers. The attacker exploited computers that were connected via a specific management system. For this type of attack, an attacker first analyzes the programs used by a specific company to find vulnerability within that program.

# Findings 3: Related Hacking Groups

Outlined below are the various types of malware and attack methods used by groups that attacked defense industry.

## 1. Icefog

This group has been active since 2011, and their main targets are government organizations and defense industry of South Korea and Japan. Vulnerabilities of MS Office, Java and WinHelp were exploited by the attacks. Even Mac-based exploits were included, as well as Windows-based exploits.

AhnLab has confirmed that variants of the malware made by *Icefog* group have been used in attacks on the defense industry. According to AhnLab, the last detected variant of the malware is *Icefog-NG*. *Icefog-NG* was first discovered on June 19, 2013. A total of 13 variants were found till October 2013; although the last development seems to have taken place in August.

The *Icefog* group has become inactive since October 2013 and no activities has been confirmed since. Whether they have permanently stopped their activities, or whether they are using a new malware is unknown.

## 2. Operation Red Dot

*Operation Red Dot* has been active from the spring of 2014 up to February 2017, and is, potentially, responsible for the hacking of Sony Pictures in November 2014. AhnLab has discovered around 100 variants of the *Escad* malware used by *Operation Red Dot*, and the variant which is believed to be the initial version was discovered in 2013. Since 2014, other attacks on websites related to the cooperation with North Korean relationships and the defense industry have been discovered. There were many similarities within the variants including the codes and filenames.

In November 2015, the email was sent to the exhibition participants pretending themselves as the host center of the exhibition. When the recipient opened the invitation file attached, a *backdoor* exploited the

vulnerability in the document application and infected the computer with *Escad*.

Since 2016, the targets of cyberattacks have broadened in scope to web hosting companies, major companies, and the media, and also the types of malware became more diversified, notably the Windows Zero-Day exploits. The last attack was documented in February 2017 but the continuation of attacks is highly likely.

## 3. Operation Ghost Rifle

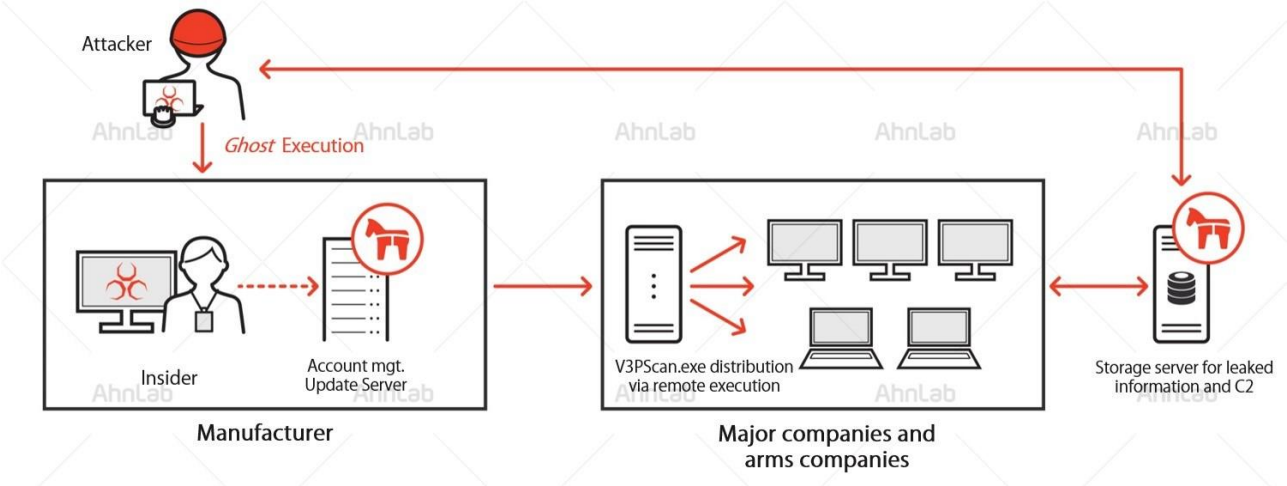
*Operation Ghost Rifle* mainly targeted the defense industry and is known to be related to the attacks of a cybersecurity company in early 2016, and a computer network of a major company in June 2016.

In the fall of 2015, the group attempted to attack companies participating in the Seoul International Aerospace & Defense Exhibition (ADEX). ADEX is an international defense industry exhibition that has been hosted bi-annually since 1996.

The attackers used emails, disguised as if sent by the exhibition host and sent attachments with vulnerabilities or excel and word documents containing malicious macros. The attachments contained information related to the exhibition so when the recipient opened the attachment and allowed *Enable Contents*, the malware infected the computer.

It has been confirmed that at least two groups were involved in this attack; *Escad* and *Rifdoor*. A variant of *Escad* was found in the attached files that exploited a vulnerability. *Rifdoor* was found in excel and word documents containing malicious macros.

In June 2016, an attack of the asset management solution of a major defense company was reported. It exploited the vulnerability of the asset management solution to distribute malware using its file distribution function, and installed a malware called *GhostRat*. Through this attack, more than 40,000 documents were reported to have been leaked.




[Figure 3] Process of the exploit of the central management program

In 2012, four years prior to this incident, the vulnerabilities of the asset management programs were discovered and the attackers attempted to attack the system since July 2017. It can be seen that a long-term preparation was made for this attack on the major companies.

## 4. Operation Anonymous Phantom

From January 2016 to October 2016, various attacks have been made on the defense industry which were based on similar malware. AhnLab named the attack Operation Anonymous Phantom based on the filename used in the initial attack phatom.exe and text string anonymous used for communication. AhnLab diagnosed this malware as Phandoor.

The malware was first discovered in January 2016 but it seems to have been created in October 2015. It targeted several defense companies but the exact attack method is yet to be confirmed. Until now, a total of 37 variants have been found and the file size varies from 76,800 to 95,232 bytes. It was also found in different names to the initial discovery, the phantom.exe file, including F_lps.exe, ahnV3.exe, v3scan.exe, otuser.exe and more.

Recently in April 2017, a variant of the malware packed as a Themida packer was found on systems in an energy research lab. In May 2017, a variant that removed the group's significant Anonymous text string was also found- indicating that the group is still active.

# Findings 4: Who is Behind the Attacks?

As mentioned earlier, multiple groups are involved in the attacks on the defense industry. As the code and encryption methods used by the *Red Dot*, *Ghost Rifle* and *Anonymous Phantom* group on the defense industry are similar to one another, there is a possibility that they are identical or cooperating group.

The encryption methods of *Rifdoor* used by *Ghost Rifle* group is similar to *Phandoor*, used by the *Anonymous Phantom* group as shown in *Figure 4*. The analysis showed similarities of the attacks around the world indicating the attack is targeting global defense industries.

```
v3 = 0x1A2C;
v4 = a1;
v11 = 0x1A2C;
result = 0x4C5B;
if ( a3 > 0 )
{
  v9 = a2 - (_DWORD)v4;
  v10 = a3;
  do
  {
    v6 = result ^ v11 & BYTE1(v3) ^ v4[v9] ^ (v3 >> 16) & HIBYTE(v3) ^ BYTE1(result) & (result >> 16) & HIBYTE(result);
    v7 = (result >> 8) | (v11 << 24);
    v3 = (v3 >> 8) | ((16 * result ^ (result ^ 2 * (result ^ 4 * result)) & 0xFFFFFFF0) << 20);
    *v4++ = v6;
    v8 = v10-- == 1;
    v11 = v3;
    result = v7;
  }
  while ( !v8 );


v4 = a2;
v5 = a2 >> 1;
v6 = 0;
v10 = v4;
v9 = v5;
v7 = result;
if ( a3 )
{
  do
  {
    *(_BYTE *)(v6 + a4) ^= v4 ^ (unsigned __int8)result;
    v8 = v5 >> 8;
    v4 = HIBYTE(result) ^ BYTE1(result) & (result >> 16) ^ v5 & BYTE1(v5) & (v5 >> 16) ^ v10 & result;
    result = (result >> 8) | (v9 << 24);
    v5 = (v5 >> 8) | (((v7 ^ (unsigned __int16)(2 * v7)) & 0x1FE) << 22);
    ++v6;
    v10 = v4;
    v9 = v8 | (((v7 ^ (unsigned __int16)(2 * v7)) & 0x1FE) << 22);
    v7 = result;
  }
  while ( v6 < a3 );
```

[Figure 4] Encryption code used in both Rifdoor and Phandoor

# Conclusion

As analyzed by AhnLab and many security companies worldwide, the attacks on the defense industry worldwide are being advanced. Since the defense industry for a country is closely related to its national security, the increase in the attacks from, potentially, a hostile country is forecasted.

Such attacks are not just a concern for private industry, but the attacks can lead to national threats, so a stronger security measure and prevention management is paramount.