
2018
GTIC MONTHLY THREAT REPORT
MAY 2018
NTT Security

# Table of Contents

## GTIC Special Report: MALSPAM

Lead researcher: Terrance DeJesus

### Introduction

GTIC security researchers have been analyzing malicious email campaigns (malspam) in recent weeks. This analysis has resulted in new discoveries of trends in tactics, techniques, and procedures (TTPs) threat actors are using to carry out these attacks. In this section of the report, GTIC researchers briefly cover what malspam is and the recent TTPs the team identified.

### What is malspam?

Malspam is a term used to describe malicious spam typically sent to a victim's email inbox. The email itself may contain a URL, which redirects the user to a spoofed or otherwise nefarious site for credential harvesting. Other types of malspam, however, contain an attachment to the email itself, with the intent of convincing the user to open the attachment. Malspam campaigns differ, but the attacker's ultimate goal is to install first-stage or final-stage malware on the victim's machine.

Threat actors cleverly craft these emails in such a way that the specific targets may be interested in opening the attachment or at least following the link. Social engineering tactics include urgent requests, banking updates and confirmations, package delivery status, delivering the malspam in the target's native language, and more.

### Recent trends in TTPs

During the most recent analysis, GTIC researchers identified malspam campaigns daily, some belonging to the same threat actor(s) and malware family, thus indicating preparation by the threat actor(s) is a continuous process.

Of the malspam campaigns analyzed, the following malware families were the most commonly observed in recent weeks. In addition to this, researchers detected Trickbot campaigns nearly every day.

| Most commonly-observed malware families |
|---|
| Emotet |
| Formbook |
| GandCrab |
| NanoCore |
| jRAT |
| Pony Fareit |
| Ursnif/Gozi |

**Figure 1.** Commonly-observed malware families

Malspam campaigns typically arrive in the morning and early evening, with the beginning and end of typical work hours in the target's time zone.

Among the analyzed malspam campaigns, the most common are those leveraging malicious attachments to install first or final-stage malware. These attachments are either in rich text format (RTF), Word and Excel documents, or Java archives (JAR). Word and Excel documents either contain several Visual Basic macros containing obfuscated strings which decode to a system command, or leverage object linking and embedding (OLE) objects to download malware. These OLE objects are also found in RTF attachments but contain exploit code for popular vulnerabilities in Equation Editor such as CVE-2017-11882 and CVE-2018-0802, which then allow system commands to be executed.

Researchers assess that the installation of exploit code for such vulnerabilities is the result of a common integration tool called ThreadKit, used for just this purpose. Threat actors will typically rotate between using OLE objects, dynamic data exchange (DDE), and obfuscated macros in their campaigns, sometimes leveraging more than one method in a single campaign.

System commands are typically specific to Windows environments. For example, PowerShell, BITSAdmin, and CertUtil commands are used in the first installation phase, after the attachment is opened.

Once installed, depending on the campaign and malware family, additional malicious binaries may be dropped or downloaded to carry out the attack. It's worth noting here that researchers found recent campaigns leveraging dynamic link library (DLL) injections into legitimate Windows processes (e.g., *svchost.exe*) during this process. Additionally, component object model (COM) objects are also loaded into the windows COM surrogate process, *DLLhost.exe*. Threat actors

***Threat actors will typically rotate between using OLE objects, dynamic data exchange (DDE), and obfuscated macros in their campaigns, sometimes leveraging more than one method in a single campaign.***

engage in these two tactics not only to make forensics analysis difficult but also to ensure the longevity of the malware payload.

The final phases of the attack are dependent on the malware family used, and the chosen malware family is often indicative of motivation of the threat actor. For example, attackers primarily use banking Trojans for data exfiltration of private information related to banking details, subsequently sending those details back to a remote command and control (C2) server. Attackers leveraging ransomware, on the other hand, place more emphasis on encrypting a victim's data and demanding a ransom. As a final example, remote access Trojans (RATs), such as NanoCore, are typically used for data exfiltration as well, and are responsible for setting up a persistent tunnel back into the victim's system. Some of the TTPs used to maintain a foothold on a victim's system may include scheduled task jobs, created or modified registry keys, and duplicates of the RAT itself.

Of the malspam campaigns analyzed, attackers do not appear to be targeting a specific industry, but rather, email addresses found in data dumps, public forums, etc., which are being used to pump out as many malspam emails as possible. This is typically achieved by a botnet, which means that any organization, entity, or individual could be a target.

It is crucial to train users to identify the signs of a malspam attack, employ a defense-in-depth security strategy, and ensure (in the case users in your organization do succumb to a cleverly crafted malspam email) backups are reliable and accessible.

---

## Spectre vulnerability back again

Lead researcher: Aaron Perkins

In January of this year, Google's Project Zero released details about undisclosed vulnerabilities in Intel's CPU chips, naming the vulnerabilities Spectre and Meltdown. The CPU hardware implementations are vulnerable to side-channel attacks, allowing an attacker to read privileged memory.

The nature of these vulnerabilities and their fixes introduces the possibility of reduced performance on patched systems. The performance impact depends on the hardware and the applications in place.

Meltdown affects Intel processors, and works by breaking through the barrier which prevents applications from accessing arbitrary locations in kernel memory.

Spectre impacts Intel, AMD, and ARM processors, broadening its reach to include mobile phones, embedded devices, and virtually anything with a chip in it. Spectre works differently from Meltdown, essentially tricking applications into accidentally disclosing information which would normally be inaccessible, safe inside their protected memory area.

As of January, there were only three variants of the Meltdown/Spectre vulnerabilities (i.e., CVE-2017-5753, CVE-2017-5715, CVE-2017-5754). As of 21 May, researchers had discovered two more.

**Variant 3a** (CVE-2018-3640) may allow an attacker to leverage side-channel analysis to obtain sensitive information. Variant 3a does require local access to the system, however.

**Variant 4** (CVE-2018-3639) has a highly complex implementation, but successful exploitation could allow an attacker to read arbitrary privileged data or run older commands speculatively. The latter would result in cache allocations which could be used to exfiltrate data.

Intel has a full list of affected products, and US CERT also published a comprehensive technical alert on these vulnerabilities.

---

## EFAIL: Big, but overhyped

Lead researcher: Aaron Perkins

In early May, security researchers discovered vulnerabilities in OpenPGP (CVE-2017-17688) and S/MIME (CVE-2017-17689). It was initially believed that these vulnerabilities, which researchers dubbed EFAIL, were vulnerabilities in the end-to-end encryption technologies OpenPGP and S/MIME, with the primary problem being that that EFAIL enabled encrypted emails to be read in plain text. Further analysis indicated, however, that the EFAIL vulnerabilities were less about vulnerabilities in the encryption protocols themselves, and more about how email clients handle messages encrypted with OpenPGP or S/MIME protocols.

One element that seemed to be overlooked was that, to set the conditions for leveraging the EFAIL vulnerabilities, the attacker must first access the encrypted emails. In other words, the attacker would need to use one or more methods to set these conditions – eavesdropping on network traffic, compromising emails accounts, servers, etc.

NTT Security researchers believe that if an attacker can successfully exploit the EFAIL vulnerabilities against a target, this action is indicative of a larger problem on the target network.

Ensuring a defense-in-depth strategy is in place across your environment is likely the best course of action to protect yourself against the EFAIL vulnerabilities. That being said, there are specific steps you can take to mitigate the risks associated with the EFAIL vulnerabilities specifically.

- **Decrypt emails with a third-party application.** The best way to prevent EFAIL attacks is to only decrypt S/MIME or PGP emails in a separate application outside of your email client.
- **Disable HTML rendering.** The EFAIL attacks abuse active content, mostly in the form of HTML images, styles, etc. Disabling the presentation of incoming HTML emails in your email client will close the most prominent way of attacking EFAIL.
- **Patch affected clients.** Check with the vendor of your email client to determine if the vendor has published patches to fix the EFAIL vulnerabilities.

**References**

Official EFAIL website
EFF Notification regarding EFAIL

---

## China's intelligence apparatus: Winnti group prepping for more attacks via the supply chain

Lead researcher: Danika Blessman

Security researchers have identified the Winnti Group, known as Axiom or APT17 in previous reporting, as likely being a conglomeration of multiple Chinese advanced persistent threat (APT) groups, all potentially associated with Chinese state intelligence services.

These groups were first reported as being potentially linked in 2013, and researchers believe the groups may have been combining efforts to some extent since 2007. At that time, separate groups had their own methods and processes, with varying technical capabilities and targets. Years of study have found that these groups were increasingly following common operational patterns, including overlapping command and control infrastructure, as well as tactics, techniques and procedures (TTPs).

Historically, the Winnti group has targeted technology firms, and this is still the case today. More recently, their TTPs appear to be evolving – or perhaps simply shifting focus.

Spear-phishing is still the ingress route of choice – collecting credentials and entering the network appearing as legitimate users to establish a foothold. The most recent spear-phishing attacks target users of both Office365 and Gmail. The attacks are aimed at IT personnel as well as HR departments.

Current operations still primarily target the technology and software sectors, although gaming, media and government sectors are also in the crosshairs in the U.S., Japan, South Korea, and China. The primary motivation of these operations seems to be theft of code-signing certificates, suggesting preparation for attacks via the supply chain using malicious versions of a valid certificate, as was observed in recent attacks targeting CCleaner, a software designed to remove unnecessary system registry files. Intellectual property, a long-time target of suspected state-sponsored Chinese threat groups, is also of value, especially internal technology documentation and source code.

***Spear-phishing is still the ingress route of choice – collecting credentials and entering the network appearing as legitimate users to establish a foothold.***

While some researchers believe identification of this group was achieved by Winnti group's sloppy operational procedures, many suspected Chinese state-sponsored threat actors have often acted brazenly, making little attempt at hiding their activities. Either way, these observations revealed overlapping infrastructure or TTPs, previously deemed unrelated.

Although researchers are still uncovering details surrounding this umbrella group, it could be that these separate groups have now combined forces, or are sharing tools and target sets. Alternatively, it could be that these groups may have historically worked as one, and researchers continue to discover similarities in indicators and TTPs during the attribution process.

Regardless, the newest Winnti umbrella operations show yet another successful campaign against a very specific target set on these organizations' supply chains.

Of note is the uptick in cyberattacks from suspected Chinese actors, suggesting a break in the anti-hacking pact between the U.S. and China. While recent agreements between the U.S. and China appear to have averted a trade war between the two countries, overall attacks targeting intellectual property are unlikely to slow.

Users are highly encouraged to be aware of all vendors in their supply chain and implement an active vendor management program, as this attack vector is becoming more commonplace.

**References**

Report: China's Intelligence Apparatus Linked to Previously Unconnected Threat Groups
Blog: CCleaner hack: what we've learned

---

### About the Global Threat Intelligence Center (GTIC)

The NTT Security GTIC protects and informs NTT Security clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures, threat reports and white papers, visit the NTT Security resource page or our blog.