DUQU 2.0:

FREQUENTLY ASKED QUESTIONS

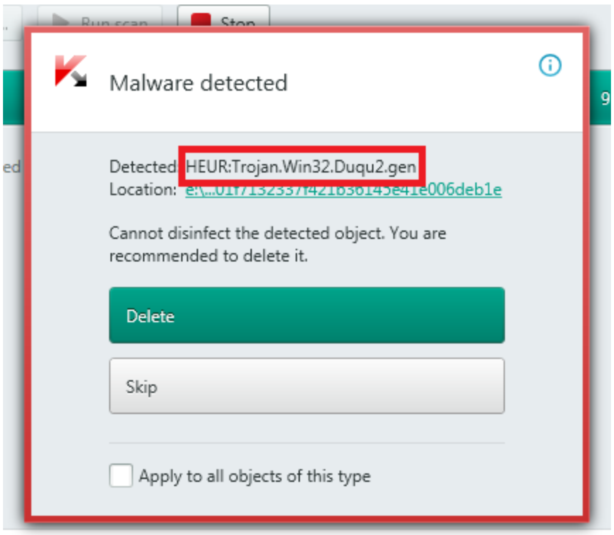
Introduction

In early spring this year, Kaspersky Lab detected a cyber-intrusion affecting several of its internal systems. We immediately launched an intensive investigation, which led to the discovery of a carefully planned cyber-espionage attack carried out by the same group that was behind the infamous 2011 Duqu APT. We believe this is a nation-state sponsored campaign.

Duqu is a sophisticated malware platform discovered by CrySyS Lab, and investigated by Kaspersky Lab in 2011. Its main purpose was to act as a backdoor into the system and facilitate the theft of private information. In 2011 Duqu was detected in Hungary, Austria, Indonesia, the UK, Sudan and Iran. There are clues that Duqu was used to spy on the Iran nuclear program and also to compromise Certificates Authorities to hijack digital certificates. These certificates were used to sign malicious files to evade security solutions.

Kaspersky Lab believes the attackers were certain it was impossible to discover the cyberattack. They did everything possible to avoid exposure: the attack included some unique and earlier unseen features and almost didn't leave any traces. The attack exploited zero-day vulnerabilities and after elevating privileges to domain administrator, the malware spread in the network through MSI files which are commonly used by system administrators to deploy software on remote Windows computers. The cyberattack didn't create or modify any disk files or system settings, making detection almost impossible. The philosophy and way of thinking of the 'Duqu 2.0' group is a generation ahead of anything seen in the APT world. But thanks to our technologies and top class researchers, we caught them.

To mitigate this threat, Kaspersky Lab is releasing Indicators of Compromise and would like to offer its assistance to all interested or affected organizations. Also, procedures for protection from Duqu 2.0 have been added to the company's products.



Malware detected

Detected: HEUR:Trojan.Win32.Duqu2.gen
Location: e:\...01f7132337f421b36145e41e006deb1e

Cannot disinfect the detected object. You are recommended to delete it.

☐ Apply to all objects of this type

More details on the Duqu 2.0 malware can be found in the technical report.

Who are the targets of this campaign?

Kaspersky Lab researchers discovered the company wasn't the only target of this powerful threat actor. Other victims have been found in Western, Middle-Eastern and Asian countries. Most notably, some of the new 2014-2015 infections are linked to the P5+1 events and venues related to the negotiations with Iran about a nuclear deal. The threat actor also launched a similar attack in relation to the 70th anniversary event of the liberation of Auschwitz-Birkenau.

Kaspersky Lab would like to reiterate that these are only preliminary results of its investigation. There is no doubt that this attack had a much wider geographical reach and many more targets. But judging from what the company already knows, Duqu 2.0 has been used to attack a complex range of targets at the highest levels with similarly varied geo-political interests.

What is the significance of this discovery?

The philosophy and way of thinking of the Duqu 2.0 group is a generation ahead of anything seen in the APT world. Its level of sophistication surpasses even the Equation Group – supposedly the 'crème de la crème' in this sphere.

The Equation Group always used some form of 'persistence, accepting a bigger risk of being discovered. The Duqu 2.0 malware platform was designed in a way that survives almost exclusively in the memory of infected systems, without need for persistence – it means the attackers are sure there is always a way for them to maintain an infection – even if the victim's machine is rebooted and the malware disappears from the memory.

That approach is much more sophisticated. It also demonstrates a different mentality: the Duqu 2.0 threat actor was confident enough to create and manage an entire cyber-espionage operation just in memory – one that could survive within an entire network of compromised computers without relying on any persistence mechanism at all.

In addition, the Equation Group used the same encryption algorithm with the same specific features in all their malware – starting with the Equation Vector in 1999 through to GrayFish in 2013. With Duqu 2.0, every single encryption is different, with different algorithms for every case.

These reasons make Duqu 2.0 more advanced than any other APT group.

What are the consequences of this cyberattack for Kaspersky Lab?

Kaspersky Lab performed an initial security audit and analysis of the attack. The analysis revealed that the main goal of the attackers was to spy on Kaspersky Lab technologies, ongoing research and internal processes. The attackers were interested in Kaspersky Lab's intellectual property and proprietary technologies used for discovering and analyzing APTs, and the data on current investigations into advanced targeted attacks; they were especially interested in our product innovations, including Kaspersky Lab's Secure Operating System, Kaspersky Security Network, Kaspersky Fraud Prevention and Anti-APT solutions. Besides intellectual property theft, no additional indicators of malicious activity were detected. Also, no interference with processes or systems was detected.

The attackers were likely aware of the company's reputation as one of the most advanced in detecting and fighting complex APT attacks, and were attempting to find ways to make their future attacks go undetected.

The information accessed by the attackers is in no way critical to the operation of the company's products. Armed with information about this attack Kaspersky Lab will continue to improve the performance of its IT security solutions portfolio.

What does this incident mean to Kaspersky Lab customers?

Kaspersky Lab is confident that its clients and partners are safe and that there is no impact on the company's products, technologies and services. The attackers' main goal was not customers' data, but access to Kaspersky Lab's intellectual property and proprietary technologies used for discovering and analyzing APTs, and the data on current investigations into advanced targeted attacks.

Kaspersky Lab would like to assure its clients and partners that the company will continue to protect against any cyberattack indiscriminately. Kaspersky Lab is committed to doing right by its customers and maintaining their full trust and confidence, and the company is confident that the steps taken will address this incident while preventing a similar issue from occurring again.

How did you discover the attack?

We detected the attack in early spring of this year. We were able to discover it thanks to the expertise of our researchers and our technologies: during a test, a prototype of an anti-APT solution developed by Kaspersky Lab showed signs of a complex targeted attack on its corporate network. After the attack was noticed an internal investigation was launched. A team of Kaspersky Lab researchers, reverse engineers and malware analysts worked around the clock to analyze this exceptional attack.

What are the reasons to think that a nation-state is behind this attack?

Developing and operating such a professional malware campaign is extremely expensive and requires resources beyond those of everyday cybercriminals. The cost of developing and maintaining such a malicious framework is colossal: we estimate it to be around $50 million. What is really remarkable here is that the entire malware platform relies heavily on zero-days. If there is no zero-day to jump into kernel mode, the malware won't work. That could mean that the attackers were pretty confident that should one vulnerability be patched they'd implement another. Otherwise they wouldn't have built a platform dependent entirely on zero-days.

The Duqu 2.0 operation displays no objective of getting any financial profit from the use of the malware.

The use of multiple zero-day exploits and sophisticated hacking techniques during the attack is another indicator that it is a nation-state sponsored campaign.

Why do you think Kaspersky Lab was targeted alongside high-level government representatives?

The targeting of Kaspersky Lab represents a huge step for the attackers and is an indicator of how quick the cyber-arms race is escalating. Back in 2011 and 2013, respectively, [1]RSA and [2]Bit9 were hacked by Chinese-speaking APT groups but these incidents were considered rare. In general, an attacker risks a lot targeting a security company – because they may get caught and exposed. The exact reason why Kaspersky Lab was targeted is still not clear – although we believe the primary goal of the attack was to acquire information on Kaspersky Lab's newest defensive technologies.

Does this attack mean that there is no protection from government-grade malware?

No, it doesn't. A conventional approach to protect endpoints may not help against professional government-grade malware. We realized this some time ago, and started developing new technologies. Our Anti-APT solution is one such technology. We discovered Duqu 2.0 while testing a prototype of our new anti-APT product.

APT attacks differ very much from the point of view of the skills of the threat actor and the resources available to launch sophisticated attacks. Unfortunately, some of these campaigns – like Stuxnet, Flame and Equation – can go undetected for several years. However, IT security companies will eventually discover these campaigns as there is no such thing as perfect code (including malicious).

Is there any reputational damage to Kaspersky Lab?

It is still believed that disclosing a cyber-incident leads to reputation damage first and foremost. In reality this is a false and dangerous conclusion and the reality is that any company can fall victim to sophisticated targeted attacks. Why is it dangerous? Because concealing such facts helps cybercriminals and government-backed hacker groups in that their malicious activities are not publicly disclosed and discussed and the data on how to prevent their attacks is not widely distributed.

By communicating the news about the incident and publishing our technical report on Duqu 2.0 we intend to send a message to other companies and encourage them to disclose details of cyberattacks on their networks. Our case shows that even a leading security company can be a target of a well-resourced APT threat actor. It is important to remember that national intelligence

[1] https://blogs.rsa.com/anatomy-of-an-attack/
[2] https://blog.bit9.com/2013/02/08/bit9-and-our-customers-security/

services can have multi-billion-dollar budgets and hundreds of thousands of employees. We can fight back by being open, transparent and by making such malicious activities public.

Kaspersky Lab has consistently advocated responsible behavior regarding disclosure of cyberattacks. We're confident that concealing security incidents leads to a situation in which less information leads to less awareness, and ultimately to weaker protection. We believe that every attacked company should disclose security incidents, which would also allow other companies to make their defenses stronger.

Is this the first time that a nation-state group has targeted an IT security company?

Unfortunately, this is not the first nation-state linked attack against a security vendor. Previous attacks against RSA Security and Bit9 were linked to nation-state attackers. Threat actors appear to compromise IT Security companies as 'utilitarian targets', which allow them to improve their cyber capabilities.

What was done to prevent this kind of attack in future?

We are taking multiple aggressive measures to further improve our IT infrastructure to protect our assets and our customers. We are trying to make it as difficult and expensive as possible for anyone to target us, from all points of view.

What mitigation strategy can you recommend?

We recommend applying the following four simple but very effective measures:

1. Make sure you have installed Kaspersky products on all the computers at your location, including servers, proxies, and any other type of computer you may have.
2. Update Windows to the latest version using Microsoft Windows Update. Make sure you install Microsoft's Patch Tuesday update from June 9, 2015.
3. Reboot all computers at once – for instance simulating a power failure. It is very important to reboot everything at the same time, otherwise the malware might survive on a machine and re-infect the others.
4. Change all passwords.

The following general strategies will help mitigate attacks with Duqu 2.0:

- Perform regular updates and rebooting of all machines in the network, including domain controllers. Rebooting removes the active malware from memory.
- Make sure all your servers run x64 (64-bit) Windows. This forces the attackers to use signed drivers for persistence mechanisms.

- Change passwords regularly (every 1-2 months) and use strong passphrases that are longer than 20 characters. Disable old-style LM hashes.

For more advanced users, we are providing Yara rules and a tool that can help identify infections in memory dumps and event logs.

In addition to these, we have published an article on Securelist "How to mitigate 85% of all targeted attacks using 4 simple strategies". We recommend reading it and implementing the suggestions in your network.

Who should I contact in case I/my company became a victim of the Duqu 2.0 campaign?

If you have any questions or information to share about this threat actor, please contact intelreports@kaspersky.com. Thank you.