Orange
Cyberdefense

Epidemiology Labs | Threat Intelligence Report

Potential risks for the pharmaceutical sector

Date: April 6 (update)

Version: 2.0

TLP: White

Authors: OSINT Unit –
Part of the Orange Cyberdefense
Epidemiology Lab

Abstract – Pharmaceutical Sector

Status	Level 2 : potential risk
Date of the report	February 28, 2020
Report modification (new elements)	April 6, 2020
Version	2.0.
Target Sectors	Pharmaceutical
Hacker Groups / Family	Winnti Umbrella APT 41 APT 10 Blacksturgeon
Suspected state actors	Mostly China Iran
Geopolitical context	Increased interest in the biopharmaceutical industry credited to threat actors likely related to/sponsored by Chinese government organisations
Hypothetical Risks on Business Lines Relationships	Several business lines could be concerned by risks (see the table p. 28)

Abstract

Pharmaceutical companies are a **prime target for hackers**, whether they are interested in intellectual property or sensitive data.

Different pharmaceutical companies have been affected by cyberattacks over the last few years, but the **goals, targets and methods employed vary**. Some are collateral damage, others are infected for spying or ransom. Regardless of the attack, the consequences can be disastrous for the company.

Among the hacker groups targeting the pharmaceutical industry, **Chinese actors seem the more active and dangerous for the sector**. All appear to have links with the Chinese state. APT41 seems particularly dangerous at that time. However, there are no hacker groups known to specifically target the pharmaceutical industry.

The recent **Chinese interest in the biopharmaceutical industry** has to be highlighted. Different U.S. government organisations have underlined the fact that biopharmaceutical companies were among the favourite industries of Chinese hacker groups looking to steal trade secrets, and that increasing Chinese **investments in the U.S. biotechnology sector represented a risk for national security**.

Contact:cyber.defense@orange.fr

Hypothesis of our OSINT Unit

Different reports and information lead us to conclude with high confidence that China is highly interested in the pharmaceutical sector. China's capabilities in cyberspace are also highly developed, whether it is under the People's Liberation Army or "state-affiliated cyber militias". As most of cyberattacks conducted against the pharmaceutical sector would emanate from Chinese hacker groups, the hypothesis that **a group of Chinese hackers could carry out a cyberattack against a pharmaceutical company is relevant, especially if this company owns manufacturing sites in the United States.**

Our hypothesis is that **APT 41** is the most active and dangerous hacker group at this time (April 6, 2020), and that in the context of the **COVID-19 outbreak**, it will go back to **espionage activities** once the quarantine is over in China. For this reason, our laboratory assesses that **patents for vaccines and COVID-19 quick detection tests are at high risk of being stolen** via cyber espionage, before being registered.

Another hypothesis is the **decredibilisation of the pharmaceutical sector** for ideological purposes, through "**cyber-hacktivism".** Anger over various conspiracy theories regarding the search for treatment for COVID-19 could lead hacktivists to launch denial-of-service attacks.

The pharmaceutical and healthcare industry is also a **difficult sector to protect**. Several threats could pose risks for these sectors, threatening data protection: a high number of M&A activities, machine learning and artificial intelligence, numerous partner industries, but also threats from within the company (third party players).

In the case of successful cyberattacks, the consequences can be disastrous for the company. Data stealing or espionage can lead to **replications of clinic trials, considerable financial loss, litigation and even dangerous consequences for clients' health**: downtime, spillage of hazardous materials, production of ineffective or toxic drugs, etc.

Recommendations

We recommend to companies in the pharmaceutical sector to **take all precautions against a possible cyberattack - which could come from Chinese hacker groups. This is even more important in the context of the COVID-19 pandemic:** cyber threat actors are trying to capitalise on this global health crisis by creating malware or launching attacks with a COVID-19 theme. Espionage concerning vaccines and COVID-19 quick detection tests is also a high risk for the pharmaceutical sector.

We recommend that companies in the pharmaceutical sector **strengthen the security of network accesses** by their partner businesses, including the **energy/chemistry, banking/finance, maintenance, manufacturing, NGOs, government, technology/telecommunications and transportation sectors.**

Contact:cyber.defense@orange.fr

Summary

1 The pharmaceutical sector is a prime target

1.1. Context

The pharmaceutical sector employs several hundred million people worldwide and is the 6th largest economic market in the world. It is both a prime target for cybercriminals and one of the most difficult sectors to protect in terms of cybersecurity.

Recent research indicates that pharmaceutical companies became the industry most targeted by cyberattacks in the last quarter of 2018, with an average of 71 fraud attacks per company[1]. In fact there were 282 attacks against the pharmaceutical industry in 2018.

“Pharmaceutical industry” refers to the economic sector that includes research, manufacturing and marketing of medicines for human or veterinary medicine. These activities are carried out by pharmaceutical laboratories and biotechnology companies.

1.2. Distribution of the pharmaceutical market

Biggest Pharmaceutical Laboratories Worldwide (Revenues), Projection for the year 2020[2]
Source : Handelsblatt (Germany), January 9, 2020

NAME	COUNTRY	REVENUES (billion USD)
Johnson & Johnson	USA	85,2
Roche	Swiss	64,9
Novartis	Swiss	49,7
Merck & Co	USA	49,3
Pfizer	USA	47,3
Glaxo-Smithkline	U.K.	46,0
Bristol-Myers Squibb	USA	42,2
Sanofi	France	42
AbbVie	USA	35,3
Astra-Zeneca	U.K.	27,0

[1]https://www.securingindustry.com/pharmaceuticals/charles-river-is-latest-pharma-co-to-face-cyber-attack/s40/a9763/#.Xlf7NKhKhhG

[2]https://www.pharmapro.ch/fr/N2768/plus-grands-laboratoires-pharmaceutiques-du-monde-chiffre-d-affaires.html

Key figures

In the United States, “Big Pharma” is employed to characterise these largest pharmaceutical laboratories in the world, with a projected turnover in 2020 of 489 billion USD for the 10 largest laboratories. Only 4 countries are represented in the list of the 10 largest pharmaceutical companies in the world: USA (5 times), Switzerland (twice), United Kingdom (twice) and France (once). Sanofi, the French group, ranks 8th in terms of revenues.

It was estimated that the pharmaceutical industry as a whole (i.e. not the top 10 companies in terms of sales) had achieved a turnover of approximately 856 billion USD in 2012[3].

1.3. A sensitive sector that attracts cyber attackers

There are three reasons for the interest of hacker groups in the pharmaceutical industry.

Firstly, there is a **profusion of intellectual property**. In the pharmaceutical sector, this can be defined as industrial property: it protects technical discoveries (patents), ornamental creations (designs) and distinctive signs (trademarks, signs, domain names, appellations of origin, etc.). In the case of medicines, it is above all a question of industrial property rights such as trademarks and patents. As a result, the theft of intellectual property concerning drugs and new compounds can be very lucrative for hackers, since the resale of the latter can be profitable on the Dark Web markets and promises very high financial rewards.

Secondly, the **sensitivity of patient data** attracts potential hackers. The flow of data in this sector is very important, especially when it comes to drug development. For example, according to the pharmaceutical company Parexel, the amount of data collected and used in regulatory submissions for 400 pharmaceutical trials amounts to approximately 160 terabytes[4]. A Reuters report indicated that the financial value of healthcare data can be as much as ten times that of a credit card number on the black market[5].

Thirdly, the pharmaceutical sector is **a controversial sector**: it mixes public health issues and commercial drivers. Given the strong links between the commercial world and the scientific world, possible conflicts of interest sometimes taint large laboratories. The *Leviator* scandals, the H1N1 vaccines in France and VIOXX in the United States have fuelled public mistrust of this sector. As a result, this sector has been targeted by whistleblowers and cyber-hacktivists. In 2016, under the banner of Anonymous, Internet users made a plea to fight the pharmaceutical business, arguing "our health is more important than their profit"[6]. Much more recently, the ransomware operator *Doppelpaymer* stated that even if they don't target hospitals in the context of the COVID-19 pandemic, they won't have mercy on pharmaceutical companies that are only interested in profit[7].This cyber hacktivist threat should therefore not be underestimated.

[3] Ibid.

[4] https://www.forbes.com/sites/yiannismouratidis/2018/11/14/billions-will-be-poured-into-ai-drug-development/#3440a0177b9f

[5] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

[6] https://www.zataz.com/anonymous-hacktivistes-tapent-sante-lemploi-a-coups-de-piratage/

[7] https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

2 Historical Zoom On Cyberattacks Targeting the Pharmaceutical Industry

2.1. Merck & co, the collateral victims of an unnamed war

In 2017, Merck & Co, a U.S. pharmaceutical company (4th worldwide in terms of revenues), was hit by the cyberattack known as "**NotPetya**". Active pharmaceutical ingredients and some R&D systems were seriously disrupted.

A screen displaying the message that files had been encrypted and asking $300 in Bitcoin per computer to retrieve them welcomed Merck's employees in June 2017[8]. In total, the attack would have paralysed more than 30,000 laptops and desktops at the drug manufacturer, as well as 7,500 servers**. Sales, manufacturing and research units were all affected.** The company was paralysed for two weeks.

What at first glance looked like a classic ransomware seems in fact to have been developed by **the Russian military intelligence agency, the GRU[9].** NotPetya's real targets would have been located in Ukraine, whose relations with Russia have deteriorated sharply since the 2014 clashes concerning Crimea. NotPetya paralysed Ukraine for several weeks, affecting government agencies, power plants, and even a Chernobyl radiation monitoring system.

Merck & Co would have been only **collateral damage of an unnamed war**: the company was contaminated by a server located in Ukraine, which launched an infected tax software called M.E.Doc, and then spread. The attack claimed many other collateral victims around the world. The US White House declared in a statement that "the Russian military launched the most destructive and costly cyber-attack in history[10]."

In total, Merck estimated at the end of 2017 that the malware had cost the company $870 million in damages. Not only did it cripple Merck's production facilities, but Merck was unable to meet the demand for some of the drugs it produced.

In the end, the pharmaceutical company turned to its insurers, since the company was covered to the tune of $1.75 billion with a $150 million deductible for "catastrophic risks including destruction of computer data, coding and software". Yet **30 of the company's insurers refused to cover the costs**[11]. They argued that the **damage caused by the cyberattack was the result of an "act of war", that was excluded in their policies**. "NotPetya" having probably been developed by the Russian intelligence services to harm their Ukrainian neighbors, Merck found itself trapped by a war in cyberspace.

[8] https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war

[9] Ibid.

[10] https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

[11] https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war

2.2. Roche & Bayer were probably infected by state-related Chinese hackers

The Swiss and German pharmaceutical companies have claimed to have been attacked by the Winnti Group, a group of hackers allegedly sponsored by the Chinese state.

The attack on Roche bears the same hallmarks as the cyberattack on Bayer. In both cases, the malware was detected on the network before it did any damage. In the case of Bayer, the malware would have been discovered on the network in 2018. The company decided to isolate and monitor it to determine its purpose, rather than removing it directly from their systems[12].

After analyzing the malware present in their networks, it was concluded to be a variant of the malware known as Winnti, which gives hackers remote access to victims' computers. Analysis of the code used in the attack reveals hallmark of a group of hackers with links to the Chinese government.

In both cases, companies claimed not to have lost sensitive data about employees, patients, customers or business partners. Bayer officials said there was no evidence of data theft or third-party compromise[13].

As a result, our OSINT Unit believes that the purpose of these cyberattacks might have been reconnaisance: a spy is sent out to explore the network, for example to determine what type of intelligence a compromise of that company or another could bring. It is a sign of a dormant attack, made to progressively infiltrate the company's networks and search for information that could be valuable to the attacker, with a view to future data theft (e.g. trade secrets), espionage or the future launch of a ransomware (encryption of data for ransom demand) or wiper (data-destruction).

However, companies from various industries such as Siemens, BASF, Henkel, Marriott or Lion Air have also been affected by the malware that attacked Roche and Bayer, making the pharmaceutical sector not a specific target[14].

2.3. Dissemination of sensitive data: the Labio laboratory case

On March 17, 2015, Rex Mundi group hackers publicly disclosed the medical data of 15,000 French people after demanding a EUR 20,000 ransom from Labio, a blood analysis laboratory[15]. This is not the first attack suffered by a health institution or organisation. This illustrates that companies in the pharmaceutical / healthcare sector run the risk of having their data publicly disclosed if they do not pay ransoms.

[12] https://healthitsecurity.com/news/pharma-giant-roche-victim-of-targeted-cyberattack-report-shows The editors at HealthITSecurity, part of the Xtelligent Healthcare Media network (an American integrated marketing solutions B2B media and event company focused on the healthcare industry), connect with security and privacy experts across the continuum of care to help readers address potential threats and adopt best practices for health data security and privacy.

[13] Ibid.

[14] Ibid.

[15] https://www.01net.com/actualites/rex-mundi-les-mysterieux-pirates-qui-extorquent-des-entreprises-francaises-649252.html. 01net is a French information website specializing in new technologies and news about high-tech products.

3 Significant hacker groups known to have targeted pharmaceutical industry

3.1. Winnti Umbrella

This group would be active since at least 2009. It initially targeted gaming companies but has since broadened its target base[16].

Some reports suggest that a number of other groups, including Axiom, APT17 and Ke3chang, are closely linked to the Winnti umbrella group[17].

Links with the Chinese state intelligence apparatus

The term “umbrella” is used by the website 401TRG, because the global entity “Winnti” consists of multiple teams/actors whose TTPs align and whose infrastructures and operations overlap[18]. The different operations would be led by separate contractor teams working towards the same objective, probably set up by the Chinese government.

The name “Winnti” was first used by Kaspersky Lab in a report from 2013. “Winnti” is now mostly used to refer to a custom backdoor used by groups under the umbrella.

“Winnti group” or “Winnti umbrella” would be associated with the Chinese state intelligence apparatus, with at least some elements located in the Xicheng district of Beijing.

Targets: from software and gaming organisations to politically aligned or technologically sophisticated organisations

The Winnti umbrella and linked groups’ primary targets are software and gaming organisations. They primarily seek code signing certificates and software manipulation, with potential financial gain being their secondary objective. Targets have been identified in the United States, Japan, South Korea, and China.

Later the group switched focus to high-level targets that are politically affiliated or technologically sophisticated. This has included Tibetan and Chinese journalists, Uyghur and Tibetan activists, the government of Thailand, and prominent international technology organisations[19].

[16] https://securelist.com/winnti-more-than-just-a-game/37029/

[17] https://attack.mitre.org/groups/G0044/

[18] https://401trg.com/burning-umbrella/. 401TRG (Threat Research Group) is the Threat Research & Analysis Team at ProtectWise, a cloud-powered Network Detection & Response (NDR) platform. ProtectWise was bought in March 2019 by Verizon, an important U.S. telecommunications company.

[19] Ibid.

Main strategies used by the hacker group

T1116	Code Signing	Winnti Group used stolen certificates to sign its malware
T1014	Rootkit	Winnti Group used a rootkit to modify typical server functionality

Winnti Group typically uses stolen certificates to sign malware and is designed to look for specific processes on the victim's computer to execute malicious code. It has also been seen in the wild using a rootkit to modify the functionality of the victim's servers. Its use on Bayer's systems indicates a sophisticated and sustained espionage campaign.

3.2. APT[20] 41

A "China nexus dual espionage and financially-focused group"[21]

According to FireEye[22], APT 41 is a "China nexus dual espionage and financially-focused group". APT41 is unique among known China-based actors, because it leverages non-public malware that is typically reserved for espionage campaigns in what appears to be activity for financial gain. Chinese state-sponsored threat groups do not usually target for explicitly financial purpose, but evidence suggests APT41 has conducted simultaneous cyber-crime and cyber-espionage operations since 2014. "APT41 espionage targeting has generally aligned with China's Five-Year economic development plans" – like other Chinese espionage operators.

Another recent report from FireEye suggests that APT 41 has carried out one of the broadest campaigns by a Chinese cyber espionage group in recent years, between January 20 and March 11[23]. FireEye adds that they did not observe APT 41 activity at their customers between February 2 and February 19. Because of the COVID-19 outbreak, quarantines in cities in Hubei province started on January 23, but additional provinces quarantines started between February 2 and February 10. The reduction in activity might therefore be related to the COVID-19 quarantine measures in China. However, APT 41 may also have been active in other ways, undetectable for FireEye at that time.

[20] APTs (Advanced Persistent Threats) are prolonged, aimed attacks on specific targets with the intention to compromise their systems and gain information from or about that target. APTs are often associated with government or military operations, as they tend to be the organisations with the resources necessary to conduct such an attack.

[21] https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html. FireEye is an American IT security company founded in 2004. It provides hardware, software and services to investigate cyberattacks, to protect against malware and to analyse computer security risks.

[22] https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

[23] https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

Targets including healthcare and pharmaceutical sector

The group has established and maintained strategic access to organisations in various sectors, including healthcare & pharmaceutical. The healthcare sector was targeted in 2014, 2015, 2016 and 2018, while the pharmaceutical sector was targeted in 2015[24].

Since the beginning of the year, the following industries were targeted: Banking/Finance, Construction, Defense Industrial Base, Government, Healthcare, High Technology, Higher Education, Legal, Manufacturing, Media, Non-profit, Oil & Gas, Petrochemical, Pharmaceutical, Real Estate, Telecommunications, Transportation, Travel and Utility.

It is unclear if APT 41 scanned the Internet and then attempted massive exploitation, or if the group targeted specifically chosen organisations. However, FireEye states that the victims appear to be more targeted in nature[25].

Attack vectors

T1015	Accessibility Features	APT41 leveraged sticky keys to establish persistence.
T1067	Bootkit	APT41 deployed Master Boot Record bootkits on Windows systems to hide their malware and maintain persistence on victim systems.
T1110	Brute Force	APT41 performed password brute-force attacks on the local admin account.
T1223	Compiled HTML File	APT41 used compiled HTML (.chm) files for targeting.
T1136	Create Account	APT41 created user accounts and adds them to the User and Admin groups.
T1486	Data Encrypted for Impact	APT41 used ransomware to encrypt files on the targeted systems and provide a ransom note to the user.
T1483	Domain Generation Algorithms	APT41 used DGA to change their C2 servers monthly.
T1133	External Remote Services	APT41 compromised an online billing/payment service using VPN access between a third-party

[24] https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

[25] https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

		service provider and the targeted payment service.
T1107	File Deletion	APT41 deleted files from the system.
T1056	Input Capture	APT41 used a keylogger called GEARSHIFT on a target system.
T1031	Modify Existing Service	APT41 modified legitimate Windows services to install malware backdoors.
T1046	Network Service Scanning	APT41 used a malware variant called WIDETONE to conduct port scans on the specified subnets.
T1135	Network Share Discovery	APT41 used the net share command as part of network reconnaissance.
T1076	Remote Desktop Protocol	APT41 used RDP for lateral movement.
T1193	Spear phishing Attachment	APT41 sent spear phishing emails with attachments such as compiled HTML (.chm) files to initially compromise their victims.
T1071	Standard Application Layer Protocol	APT41 used DNS for C2 communications.
T1195	Supply Chain Compromise	APT41 gained access to production environments where they could inject malicious code into legitimate, signed files and widely distribute them to end users.
T1049	System Network Connections Discovery	APT41 used the netstat command as part of network reconnaissance. The group has also used a malware variant to enumerate active RDP sessions.
T1078	Valid Accounts	APT41 used compromised credentials to log on to other systems.
T1047	Windows Management Instrumentation	APT41 used WMI in several ways, including for execution of commands via WMIEXEC as well as for persistence via PowerSploit

APT 41 is known to move laterally within targeted networks, by moving between Windows and Linux systems for instance, until it can access game production environments. From there, the group steals source code and digital certificates, used to sign malware.

Supply chain compromise tactics have also been characteristic of APT41's most known and recent espionage campaigns - by using its access to production environments to inject malicious code into legitimate files which are later distributed to victim organisations.

APT 41 limits the deployment of follow-on malware to specific victim systems by matching against individual system identifiers. These multi-stage operations restrict malware delivery only to targeted victims and "obfuscate" the intended targets[26] (in a normal spear-phishing campaign, the targeting can be discerned from recipients' email addresses).

According to FireEye, 46 different malware and tools are used by APT 41: publicly available utilities, own tools, and malware shared with other Chinese operations.

Strategic intelligence collection

The combination of supply chain compromises to target selected individuals, consistent signing of malware using compromised digital certificates, and deployment of bootkits (which is rare among Chinese APT groups), shows that APT 41 is a well-resourced and skilled group.

The group focused on direct intellectual property theft until 2015, then has seemed to move towards "strategic intelligence collection"[27]. The group seems to navigate between targeting for financially motivated reasons and state-sponsored operations. This may indicate the group is either protected by some authorities (so that they can continue their own for-profit activities), ignored by authorities, or that they have simply evaded scrutiny from Chinese authorities. Anyway, this shows that the boundary between crime and state-sponsored operations is thin.

3.3. APT 10

APT-10 has targeted at least 45 U.S. companies, including a few in the healthcare and biotechnology sectors.

Targets

First observed in 2009, APT10 appears linked to the Chinese Ministry of State Security (MSS). This agency usually attacks intelligence targets surrounding "trade negotiations, research and development in competition with Chinese commercial entities, and high value counter intelligence targets overseas"[28].

This Chinese cyber espionage group has historically targeted construction, engineering, aerospace, telecom firms, and governments in the United States, Europe, and Japan. These attacks appear to support Chinese state-interests, including acquiring valuable military and intelligence information and the theft of confidential business data to support Chinese corporations.The healthcare, biothechnology and pharmaceutical sectors are not a prime target of APT 10, but the group has

[26] https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

[27] Ibid.

[28] https://blog.malwarebytes.com/cybercrime/2019/01/advanced-persistent-threat-files-apt10/. Malwarebytes Inc. is an American Internet security company, specialised in protecting home computers, smartphones, and companies.

targeted them before. Although the threat on these sectors is not high, we chose to highlight this group because of the U.S. alert on biopharmaceutical companies concerning China (section 5)[29].

Attack vectors

APT 10 operations usually include both traditional spear phishing and access to victims' networks through managed service providers. APT10 spearphishing has been relatively unsophisticated, leveraging .lnk files within archives, files with double extensions and in some cases identically named decoy documents and malicious launchers within the same archive[30].

Two Chinese hackers belonging to APT 10 - Zhu Hua and Zhang Shilong - have been charged with global computer intrusion campaigns targeting intellectual property and confidential business information by the U.S. Department of Justice. The charge states that they "acted in association with the Tianjin State Security Bureau and engaged in Global Computer Intrusions for more than a decade, continuing into 2018, including thefts from managed service providers and more than 45 technology companies"[31].

3.4. BLACKSTURGEON (aka APT 33, Shamoon/Shamoon 2, Rocket Kitten, Elfin)

BLACKSTURGEON is a suspected group of Iranian hackers that has been operating since at least 2013[32]. The group has targeted organisations from several sectors, including organisations in the fields of research and health, chemicals and engineering. The majority of the targets have been located in the United States, Saudi Arabia and South Korea, with a particular interest in the aviation and energy sectors.

The group has attacked at least 50 organisations and it is specialised at searching vulnerable websites to identify potential targets, whether for attacks or C&C infrastructure. Analyzing the observed TTPs, this threatening player seems very similar to the Iranian hacker group Muddy Water.

[29] See p.19.

[30] https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

[31] https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

[32] https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

4 Highlight on significant malware that has targeted the pharmaceutical sector

4.1. Shadowpad

Active since 2017, ShadowPad spreads through trojanised software installers. Its purpose is remote control and this malware is an example of the dangers posed by a successful supply-chain attack. Given the opportunities for covert data collection, attackers are likely to pursue this type of attack again and again with other widely used software components[33].

This malware has attacked a wide range of sectors, including construction, manufacturing, financial institutions, media, energy, heavy industry manufacturers and others… but most importantly the medical industry[34].

Attribution is uncertain and attackers were, according to Kaspersky, very careful to not leave obvious traces. However, certain techniques were known to be used by other malware like PlugX and Winnti, which were allegedly developed by Chinese-speaking actors.

4.2. Blue Termite

Active since 2013, Blue Termite spreads through exploits, social engineering and watering hole attacks. Its purpose would be cyberespionage, data wiping and surveillance[35]. Its targets are wide (education, financial institutions, government entities, media, manufacturing, satellite operators…), but it also includes the Chemical Industry, Health Insurance Services, Medical Industry and Pharmaceutical.

According to Kaspersky the malware contains Chinese language artefacts[36].

4.3. Winnti

As discussed in section 3.1.[37], this malware was developed by the “Winnti umbrella” group. In 2015 Kaspersky revealed that the Winnti group had begun targeting pharmaceutical companies, possibly for industrial espionage, suggesting that they had evidence of an attack on a "well-known global pharmaceutical company headquartered in Europe”[38]. It is however suspected that the Winnti malware may have been used by another group. Typically, the trojan arrives at a network endpoint via a compromised PDF file, which can bypass firewall protection, create user folders and accounts, and inject processes with malicious payloads, and then sends information to hackers.

[33] https://apt.securelist.com/#!/threat/1584

[34] Ibid.

[35] https://apt.securelist.com/#!/threat/1010. SecureList is the “Reports and research on cyberthreats” website from Kaspersky.

[36] Ibid.

[37] See p.11.

[38] https://securelist.com/games-are-over/70991/

5 U.S. Alert on biopharmaceutical companies concerning china

Our research detailed in section 3 of this report highlights the predominance of Chinese groups in attacks against the pharmaceutical industry.

We therefore conducted further analysis of the **potential "Chinese threat**" on this sector. A few reports caught our attention.

Biopharmaceutical companies among 10 industries targeted by Chinese hackers to steal trade secrets

The U.S. Department of Homeland Security has stated that biopharmaceutical companies were among 10 industries targeted by Chinese hackers to steal trade secrets, with hackers actively exploiting relationships between IT service providers and their customers[39]. In March 2019, a survey found that more than two-thirds of U.S. organisations believed their cyber security teams are understaffed[40].

This alert followed the Department of Justice indictment of the two Chinese hackers that were accused of a global hacking campaign to steal data and technology secrets.

Increasing investments in the U.S. biotechnology sector: a risk for national security

China has rapidly increased its investment in the U.S. biotechnology sector in recent years, potentially giving them access to genetic, private and medical data. According to the US-China Economic and Security Review Commission, this could pose a risk to national security[41].

Furthermore, some researchers have determined that the Chinese government has recognised the value of healthcare-related data in the development of biotechnology and has made collection of it a national priority with four major health data centres[42].

Chinese regulators have accelerated genomics research and "in some cases bypassed the lengthy formal drug review process"[43]. The report determines that **China's large investments in U.S. biotechnology, including access to genomic data, could pose a risk to national security**, and states " China is pursuing a comprehensive, long term strategy to become a leader in biotechnology, creating globally competitive domestic firms and incentivizing the relocation of biotechnology manufacturing, design, and operations to China".

These different reports and information lead us to conclude that China is highly interested in the pharmaceutical sector. As most of cyberattacks conducted over this sector would emanate from Chinese hacker groups, **we therefore caution pharmaceutical companies that cyberattacks might come from China-sponsored hacker groups**.

[39] https://www.securingindustry.com/pharmaceuticals/charles-river-is-latest-pharma-co-to-face-cyber-attack/s40/a9763/#.XlefbKhKhhE

[40] Ibid.

[41] https://www.uscc.gov/sites/default/files/Research/US-China%20Biotech%20Report.pdf

[42] https://healthitsecurity.com/news/government-report-finds-china-could-use-medical-data-for-blackmail

[43] Ibid.

6 Chinese capabilities in cyberspace

Given the potential "Chinese threat" on the pharmaceutical sector, proceed to highlight the Chinese hacking capabilities in cyberspace. One unit in particular is relevant because it has been alleged to be a source of Chinese computer hacking attacks.

PLA Unit 61398

PLA Unit 61398 would be the "**Military Unit Cover Designator**" of an advanced persistent threat unit belonging to the People's Liberation Army, believed to be located in Shanghai (Pudong).

On May 19, 2014, five "61388" officers were charged in the U.S. for **theft of confidential business information and intellectual property from U.S. commercial firms and for planting malware** on their computers.

PLA Unit 61398 operates under the 2nd bureau of the People's Liberation Army General Staff Department Third Department. According to the computer security firm Mandiant[44], there is evidence that PLA Unit 61398 **contains, or is itself, an entity that is part of the advanced persistent threat that has attacked a broad range of corporations and government entities** around the world since at least 2006. This entity would be **one of more than 20 APT groups linked to the Chinese state**. The Third and Fourth Department are responsible for electronic warfare and would include PLA units mainly responsible for infiltrating and manipulating computer networks[45].

The collective has **stolen trade secrets and other confidential information** from several foreign businesses and organisations over the last 7 years, including Lockheed Martin, Telvent, and other companies in shipping, aeronautics, energy, engineering, manufacturing, arms, financial, electronics and software.

In May 2019, the U.S. Department of Defense's (DOD) report to Congress on China's military capabilities described a **rapidly modernising People's Liberation Army and its growing ability to exploit cyberspace** to counterbalance the traditional advantages of its peer rivals.

Accused Chinese hackers including Unit 61398 abandon techniques after U.S. indictments

U.S. indictments against individual Chinese soldiers accused of hacking various American targets would have deterred those military personnel from conducting the same kinds of hacks again, according to Dmitri Alperovitch (co-founder of CrowdStrike)[46].

This **"name-and-shame" strategy** dates back to a 2014 indictment against a Chinese hacking crew. It appears that unsealing the indictment depends on how likely U.S. Justice Department believes that the defendants will travel to a place where they c

an be arrested and extradited: if this may happen within a reasonable timeframe, the name will be kept under the seal. If it is unlikely, unsealing the names may be a good deterrant to stop the defendants pursuing their operations.

To illustrate this, digital infrastructure linked with alleged hackers charged in 2014, 2017 and 2018 essentially "evaporated" when charges in each case were made public. The four groups of hackers

[44] Now a FireEye subsidiary.

[45] https://en.wikipedia.org/wiki/PLA_Unit_61398#cite_note-huffingtonpost_professional-12.

[46] https://www.cyberscoop.com/china-pla-hacking-indictment-deterrence/. CyberScoop, a ScoopNewsGroup (an american public sector tech media company) property, reports on news and events impacting technology and security. It reaches top cybersecurity leaders both online and in-person through a website, newsletter, events, radio and TV.

have been associated with Chinese intelligence services or the PLA, **including the Unit 61398 and the APT 10 group**. While other Chinese groups have mostly remained active, the specific groups named in the indictments disappeared in a way that was, according to Alperovitch, "remarkable"[47]. **Some of the hackers may have been re-assigned to other units that had not been publicly identified and thus may continue to launch cyberattacks for the Chinese state**. But according Alperovitch, the hackers at least had to "**reset and re-tool**". This differentiates Chinese hackers from Iranian and Russian ones, who usually do not change anything after an indictment.

Recently, the PLA "has not carried out attacks with the same high tempo as China's MSS"[48]. This dates back to the 2015 agreement between Barack Obama and Xi Jinping, under which neither nation would hack the other for commercial gain. This was followed by a quieter period, yet China's MSS emerged as a more active entity. This coincides with a re-organisation inside the army.

Note that the Chinese government has consistently denied carrying out any cyberattacks.

"State-affiliated cyber militias"[49] and APT groups

"State-affiliated cyber militias" have been one of the clearest products of China's civil-military development efforts since these organisation emerged around 20 years ago, with a membership base believed to contain more than **10 million people today**[50].

These militias could undermine the work of regular PLA units if they operated as they wished. Consequently they will likely perform **cyber-surveillance and espionage** – and not offensive cyber-operations.

Thus, APT groups that have targeted pharmaceutical companies operate within a **global organisation of APT groups originating from China** that re-organise and evolve over the years and as their existence is potentially revealed.

[47] Ibid.

[48] The Ministry of State Security (MSS) is the intelligence, security and secret police agency of the People's Republic of China (non-military area of interests), responsible for counter-intelligence, foreign intelligence and political security.

[49] https://asianmilitaryreview.com/2020/01/china-broadens-cyber-options/. Asian Military Review is the largest circulated and only audited (ABC certified) defence magazine in Asia & Pacific region, based in Bangkok, Thailand.

[50] Ibid.

7 Threat summary

To conclude this report, we would like to focus the attention of pharmaceutical companies on the following points:

Pharmaceutical companies are a **prime target for hackers**, whether for intellectual property or sensitive data.

Different pharmaceutical companies have been affected by cyberattacks over the last few years, but the **goals, targets and methods employed vary**. We've chosen to highlight three types of cyberattacks that seem relevant to us: a state-sponsored attack that made a pharmaceutical company a collateral victim, a state-related attack that was discovered in time but was probably for espionage purposes and aimed at stealing data, and a last one that was a typical ransomware attack, with sensitive healthcare data at stake.

Among the hacker groups targeting the industry, **Chinese actors seem the more active and dangerous for the sector**. They all seem to have links with the Chinese state. The recent increase in the activity of APT 41 shows how resourceful and quick they are.

The recent **Chinese interest in the biopharmaceutical industry** needs to be highlighted. Different U.S. organisations underlined the fact that the biopharmaceutical industry was amongst the favourite targets of Chinese hacker groups to steal trade secrets, and that increasing **Chinese investments in the U.S. biotechnology sector represented a risk for national security**.

These different reports and information lead us to conclude that China is highly interested in the pharmaceutical sector. **China's capabilities in cyberspace are also highly developed**, whether it is under the People's Liberation Army or "state-affiliated cyber-militias".

As most of cyberattacks conducted against the pharmaceutical sector would emanate from Chinese hacker groups, the hypothesis that **a group of Chinese hackers could carry out a cyberattack against a pharmaceutical company is relevant, especially if this company owns manufacturing sites in the United States**.

A difficult sector to protect: potential threats on the pharmaceutical sector

Health industry businesses appear to be bad students in the fight against hacking, so it is **one of the most fragile industrial sectors in terms of cybersecurity** and attacks against this industry have increased more quickly than elsewhere[51]. In 2015 one in four drug manufacturers had already been the victim of computer attacks. This figure has continued to increase since.

Furthermore, **M&A activities** are very important in this sector and an additional obstacle to data protection. As each acquisition involves the absorption of a large volume of data by the parent company, access routes, rights and permissions will all change during the process[52].

In recent years, the development of drugs by using **machine learning and Artificial Intelligence** (AI) has also increased. As these systems become integrated into production methods the exposure

[51] https://www.securingindustry.com/pharmaceuticals/survey-reveals-data-breaches-hitting-pharma-industry/s40/a2500/#.Xlj7QKhKhhG

[52] https://www.silicon.fr/avis-expert/protection-des-systemes-it-une-priorite-pour-le-secteur-de-la-sante. Silicon.fr is a French website on IT news for IT and telecom decision-makers. Every day, it offers a selection of articles, files and interviews on information technology, telecommunications and the digital society.

of new access points is inevitable. This creates a new category of critical data that could be lost outside the company, either by mistake or maliciously.

Despite the protection of data, **a large part of the risks involved emanate from within the companies themselves**. 77% of attacks are based on file-less techniques in their data capture efforts. For example, rather than launching a large-scale phishing attack on a large number of targets, companies are more likely to fall victim to attacks that seek to exploit vulnerabilities already present in their infrastructure[53].

The pharmaceutical market relies on **third party players**, such as clinical research organisations that support drug manufacturers, who in turn rely on data research facilities, project management teams and various testing and trial services. This increases the number of roleplayers and thus the risks of intellectual property theft by internal corporate actors.

Finally, the **pharmaceutical sector has a lot of relationships with other industries**. This also increases the risk of an attack due to cyber connections with a compromised partner (see p. 27-28).

Consequences are potentially disastrous

Stolen data concerning **clinical trials,** if leaked on the Dark Web or bought by hackers, **means the trials can be replicated** by other unscrupulous laboratories.

In the pharmaceutical industry the integrity of the components used depends on the strict control of hundreds of variables, from the amount of chemicals in the mixture and the mixing times, to the temperature and humidity levels of the manufacturing environment. Ensuring product quality is a major concern. Whilst cybercriminals are most often looking for intellectual property, a breach of a computer system could also lead to even more serious consequences: **downtime, production of ineffective or toxic drugs, spillage of hazardous materials**, etc[54].

For the health industry a cyberattack could result in **considerable financial loss**: shutting down production and restoring infected systems, stealing of years of research on a new drug, or damaging company's image because of a leak of sensitive data can result in colossal losses.

A successful cyberattack leading to a major data leak can also lead to penalties or **litigation[55],** particularly in the context of GDPR (for instance, in the case of an insufficient protection of the clients/patients' data). Clients or patients may also take legal recourse.

Finally, a specific risk must be underlined: the possibility of exclusions from insurance. In this respect, the case of the cyberattack against the pharmaceutical giant Merck & Co in 2017 is emblematic[56].

[53] Ibid.

[54] https://www.pharmamanufacturing.com/articles/2017/protecting-pharmaceutical-manufacturing-processes-against-cyber-threats/

[55] Ibid.

[56] See p. 8.

8 Hypothesis of our OSINT unit (April 6, 2020)

Hackers are taking advantage of this period of international health crisis during which security services are saturated and the economy is slowing down worldwide (1/3 of the world's population being confined), seeking to exploit vulnerabilities already present in the infrastructure of a relatively poorly protected sector.

Hackers could **now** take action by:

H1: **Targeting intellectual property or sensitive data for espionage** (most likely)

In this hypothesis, APT 41 would be the most active group. Targeted companies would be particularly those related to the search for a vaccine against COVID-19 or for COVID-19 quick detection tests. The biopharmaceutical industry sector is at high risk.

H2: **Discrediting the pharmaceutical sector for ideological purposes** through cyberhacktivism (least likely)

In this hypothesis, the entire pharmaceutical sector could be the target of calls for attacks of opportunity. Groups such as *Anonymous* or others could be active in this context. Furthermore, anger over various conspiracy theories regarding the search for treatment for COVID-19 could lead hacktivists (such as Anonymous) to launch denial-of-service attacks (DoS attacks).

9 Recommendations of our OSINT unit

We recommend to companies in the pharmaceutical sector to take all precautions against a possible cyberattack - which could come from Chinese hacker groups - and especially from APT 41.

This is even more important in the context of the COVID-19 pandemic. Cyber threat actors are trying to capitalise on this global health crisis by creating malware or launching attacks with a COVID-19 theme.

Due to the large number of partner industries in the pharmaceutical sector, we created the sheet below (p.27) based on our **assumptions regarding relationships with subcontractors and partners**. Risks that pharmaceutical companies need to take into account include email communication (spear phishing), file transfers and confidential meeting listening.

Pharmaceutical companies should be warned that:

- If a pharmaceutical company has connections with a company in the **energy/chemistry, banking/finance, maintenance, manufacturing or non-governmental organisations sectors,** the risk of a cyberattack affecting one of these companies impacting the pharmaceutical company is estimated to be **high.**

- If a pharmaceutical company has connections with a company in the **government, technology/telecommunications or transportation sectors**, the risk of a cyberattack affecting one of these companies company impacting the pharmaceutical company is estimated to be **quite high**.

- If a pharmaceutical company has connections with a company in the **defense/aerospace, retail/e-commerce, education and agriculture sectors**, the risk of a cyberattack affecting one of these companies impacting the pharmaceutical company is estimated to be **medium**.

We recommend that companies in the pharmaceutical sector **strengthen network security accesses** by their partner businesses, including the **energy/chemistry, banking/finance, maintenance, manufacturing, NGOs, government, technology/telecommunications and transportation sectors.**

Risk-assumptions about the partner business lines with which a company in the pharmaceutical sector could have cyber connections

Business lines	Level of technology communication with the business line studied (pharmaceutical)	"Known-level" of cybersecurity of the business line	Potential targeting risk assumption
Defense/Aerospace	Important	High	Medium
Government	Important	High	Quite high
Technologies/Telecommunications	Important	High	Quite high
Energy/Chemistry	Important	High	High
Banking/Finance	Important	High	High
Maintenance	Important	Quite medium	High
Retail/e-commerce	Medium	Quite high	Medium
Education	Medium	Weak	Medium
Construction	Weak	Weak	Weak
Transportation	Important	Medium	Quite high
Manufacturing	Important	Weak	High
Agriculture	Medium	Weak	Medium
Tourism	Weak	Weak/Medium	Weak
Non-Governmental Organisations	Important	Weak	High
Press	Weak	Weak	Weak

10 Appendices

10.1. Selected repository for the classification of sources and information

Reliability of the Source	
A	Completely reliable
B	Usually reliable
C	Fairly reliable
D	Rarely reliable
E	Unreliable
F	Reliability not estimable

Information Veracity	
1	Corroborated by other sources
2	Probably true
3	May be true
4	Doubtful
5	Unlikely
6	Unquantifiable truthfulness

10.2. Likelihood Matrix

				Veracity			
		Corroborated	Probably true	May be true	Doubtful	Unlikely	Unquantifiable truthfulness
Reliability		1	2	3	4	5	6
Completely reliable	A	Dangerous					
Usually reliable	B		High				
Fairly reliable	C			Medium			
Rarely reliable	D				Weak		
Unreliable	E					Very Weak	
Reliability not estimable	F						Not estimable

The combination of the reliability of the source and the veracity of the information allows to estimate the probability of an incident to occur, given a context.

10.3. Disclaimer

Orange Cyberdefense strives to ensure the accuracy of the information gathered in this document, but no warranty, express or implied, can be given.

Orange Cyberdefense disclaims any liability for errors or omissions resulting from/related to the use of the information and material in this document.

Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.