An abstract graphic on the left side of the slide, consisting of a complex network of white lines connecting numerous small white dots, resembling a molecular structure or a data network, set against a dark background.

# The group that wasn't – tracking and defining Winnti

---

Kamil Bojarski – X33fcon 2023

# Agenda

- Whoami
- How we define groups.
- Timeline of disclosures and evolution of the group.
- Making your own Winnti.

whoami

- Principal Intelligence Analyst at QuoIntelligence
- Teaching Assistant for SANS FOR578
- You can read my musings on security and intelligence at [counterintelligence.pl](http://counterintelligence.pl)
- Feel free to reach me:  
[Kamil.bojarski@quointelligence.eu](mailto:Kamil.bojarski@quointelligence.eu), [kamil.bojarski@lawsec.net](mailto:kamil.bojarski@lawsec.net)  
[@lawsecnet](#), [@lawsecnet@infosec.exchange](mailto:@lawsecnet@infosec.exchange)



shame

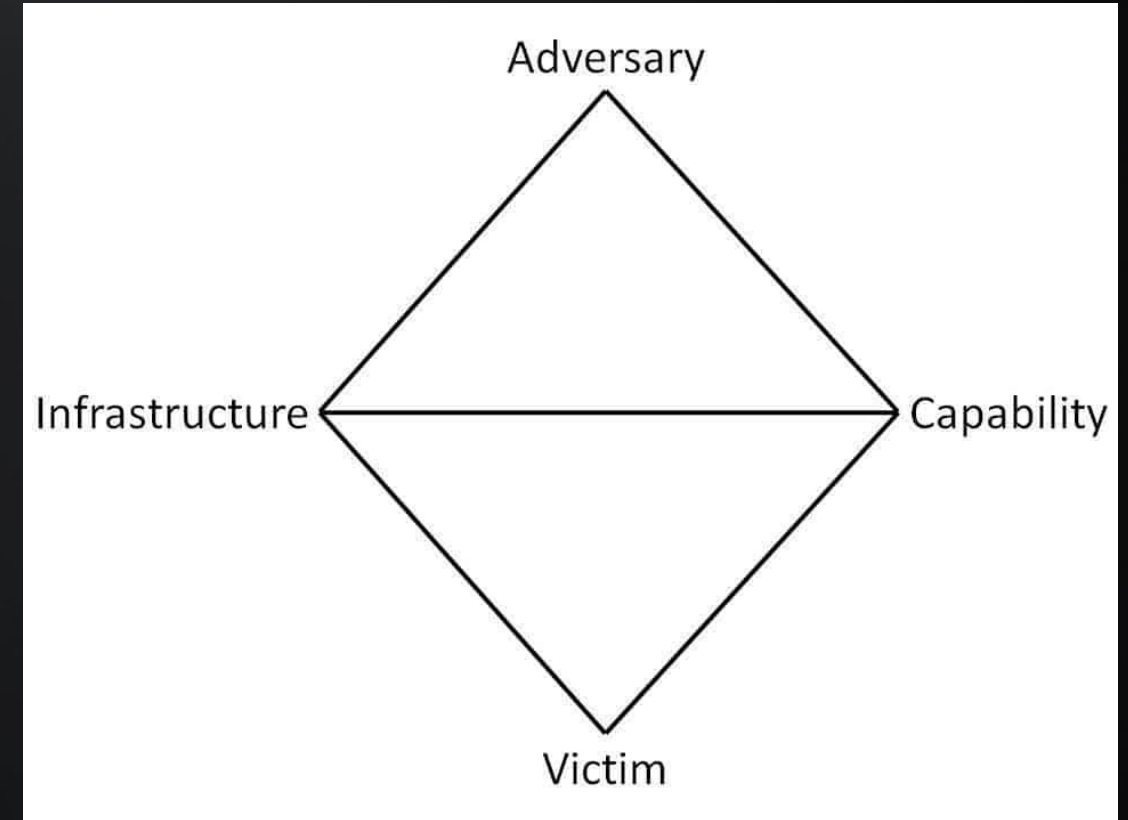


name

# Winnti – who or what?



VS



Winnti



## Winnti for Windows

[Winnti for Windows](#) is a modular remote access Trojan (RAT) that has been used likely by multiple groups to carry out intrusions in various regions since at least 2010, including by one group referred to as the same name, [Winnti Group](#).<sup>[1][2][3][4]</sup> The Linux variant is tracked separately under [Winnti for Linux](#).<sup>[5]</sup>

ID: S0141

① **Type:** MALWARE

① **Platforms:** Windows

**Version:** 3.0

**Created:** 31 May 2017

**Last Modified:** 20 March 2023

## Winnti for Linux

[Winnti for Linux](#) is a trojan, seen since at least 2015, designed specifically for targeting Linux systems. Reporting indicates the winnti malware family is shared across a number of actors including [Winnti Group](#). The Windows variant is tracked separately under [Winnti for Windows](#).<sup>[1]</sup>

ID: S0430

① **Type:** MALWARE

① **Platforms:** Linux

**Version:** 1.0

**Created:** 29 April 2020

**Last Modified:** 01 July 2020

# Winnti - timeline

- Kaspersky first names the group in 2013:
- "Symantec appears to be the first to name these malicious programs; we kept Symantec's name - Winnti - in the name of the malware family we created: Backdoor.Win32(Win64).Winnti. As for the people behind these attacks involving this remote administration tool, we ended up calling them "the Winnti group".
- Mentions already use of stolen certificates and links to intrusion against Tibetan and Uygur activists.
- Link: Malware grouping

## Winnti. More than just a game

APT REPORTS

11 APR 2013

⌚ 13 minute read



### // AUTHORS

Expert GREAT

Kaspersky Lab began this ongoing research in the autumn of 2011. The subject is a series of targeted attacks against private companies around the world.

In the course of our research we uncovered the activity of a hacking group which has Chinese origins. This group was named "Winnti".

## Winnti - timeline

- In 2013 FireEye publishes a report on the sharing of capabilities among Chinese groups. Winnti is referenced per the Kaspersky reporting.
- Link: Stolen certificates reuse.



### SUPPLY CHAIN ANALYSIS:

From Quartermaster to SunshopFireEye

During our research, we found six digital certificates used to sign 44 different malware samples. These certificates are currently revoked or expired and were signed by Microsoft, Sinacom, Facesun.cn, Mgame Corp, Guangzhou YuanLuo Technology Co., Ltd., and Wuhan Tian Chen Information Technology Co., Ltd. The full details of these certificates are available in Appendix A. According to Kaspersky, the Mgame Corp. and Guangzhou YuanLuo Technology Co., Ltd. certificates were stolen.<sup>5</sup> Whether the remaining certificates were also stolen—or were ever valid—is unclear.

# Winnti - timeline

- In 2014 cooperating companies published a report on the Chinese espionage operation.
- In 2015 supplementary report that describes Winnti malware found during analysis.
- „Novetta has moderate to high confidence that the organization-tasking Axiom is a part of Chinese Intelligence Apparatus.“

## Operation SMN:

Axiom Threat Actor Group Report  
公理队

## WINNTI ANALYSIS


As part of Operation SMN, Novetta analyzed recent versions of the Winnti malware. The samples, compiled from mid- to late 2014, exhibited minimal functional changes over the previous generations Kaspersky reported in 2013.<sup>1</sup> What is of note, however, is the increased scrutiny found within the Winnti dropper component that attempts to frustrate analysis of the malware.

# Winnti - timeline

- In 2015 Kaspersky publishes another report on the Winnti group.
- Link Winnti to Axiom group.
- Claims that newly discovered samples belong to the family described in the SMN report.
- Link: Malware grouping

**Games are over: Winnti is now targeting pharmaceutical companies**

APT REPORTS 22 JUN 2015 2 minute read



**AUTHORS**

DMITRY TARAKANOV

**GREAT WEBINARS**

13 MAY 2021, 1:00PM  
**GrEAT Ideas. Balalaika Edition**  
BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM  
**GrEAT Ideas. Green Tea Edition**  
JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM  
**GrEAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots**  
MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU, KURT BAUMGARTNER, DAN DEMETER, YAROSLAV SHMELEV

26 AUG 2020, 2:00PM

In April [Novetta released its excellent report on the Winnti malware](#) spotted in the operations of [Axiom group](#). The Axiom group has been presented as an advanced Chinese threat actor carrying out cyber-espionage attacks against a whole range of different industries. For us, the Novetta report was another source of intelligence that Winnti was already expanding beyond online games. One of the recent Winnti samples we found appears to confirm this as well.

# Winnti - timeline

- In 2016 Symantec publishes blog on the espionage operation attributed to China and using custom malware and stolen certificates.
- Indirectly references Kaspersky research.
- Link: malware and stolen certificates.

## Suckfly: Revealing the secret life of your code signing certificates

Mar 15, 2016 09:00 AM



Jon  
DiMaggio



View the [indicators of compromise](#) for this attack group.

In April 2013, a third-party vendor published a report about a cyberespionage group using custom malware and stolen certificates in their [operations](#). The report documented an advanced threat group they attributed to China. Symantec tracks the group behind this activity as Blackfly and detects the malware they use as [Backdoor.Winnti](#).

# Winnti - timeline



# Winnti - timeline

- In 2016 Blackberry/Cylance publishes research on a PassCV group and links it to Winnti.
- Link: malware and stolen certificates – association through victimology revealed by Kaspersky.

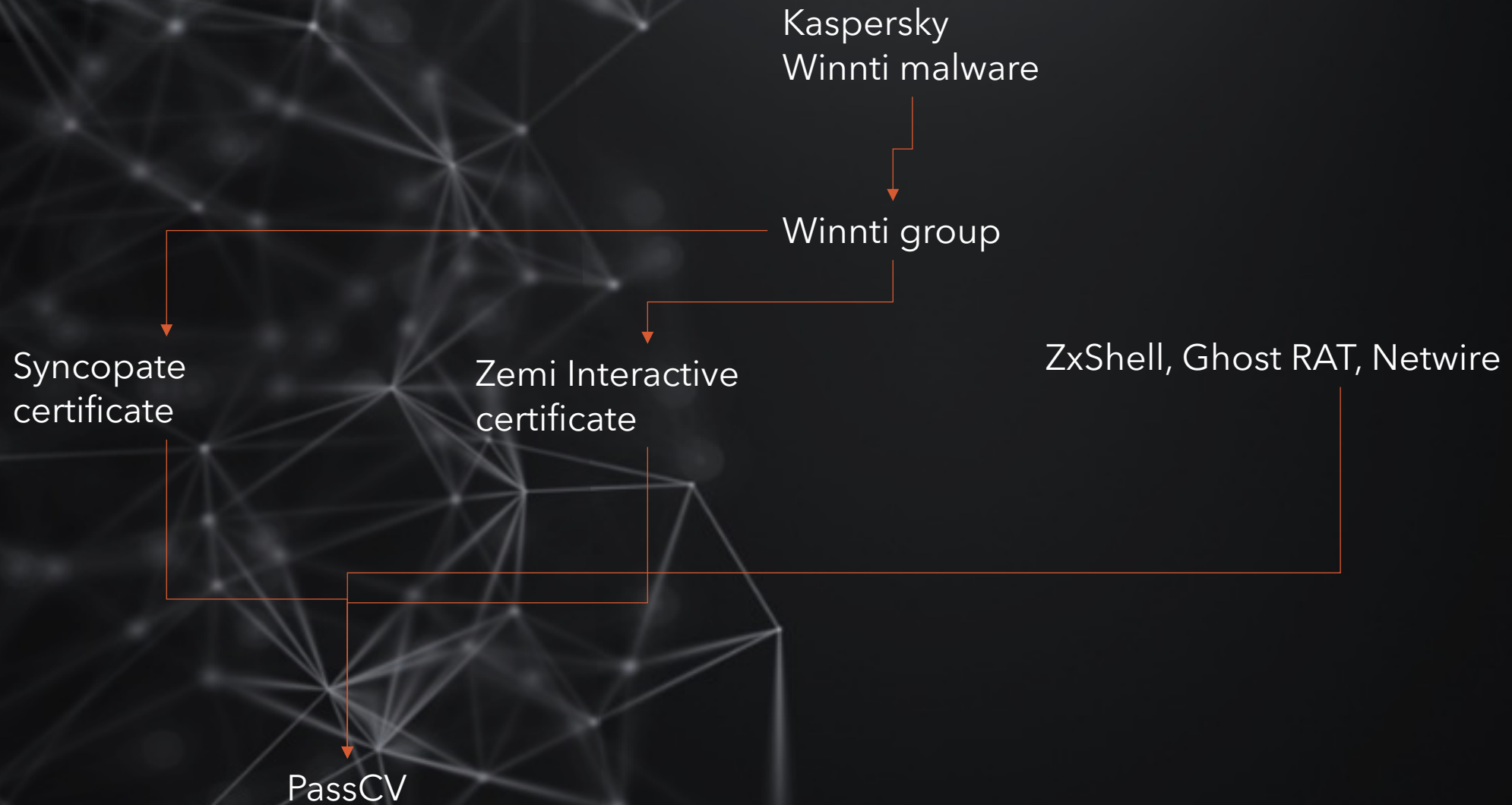
## Digitally Signed Malware Targeting Gaming Companies

RESEARCH & INTELLIGENCE / 10.18.16 / The BlackBerry Cylance Threat Research Team



Syncopate is a well-known Russian company that is best known as the developer and operator of the 'GameNet' platform. [GameNet was first identified as being a likely victim of the Winnti group here](#), although no associated code-signing certificates were identified at that time. Similarly, in that same blog post 'Zemi Interactive' was also identified as being a likely victim from the same attacks. The evidence presented above strengthens the claim that the **Winnti** and PassCV groups are closely related.

# Winnti - timeline



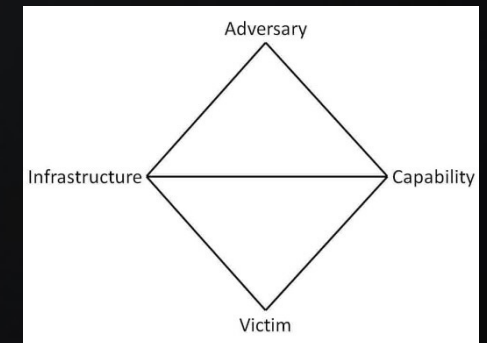
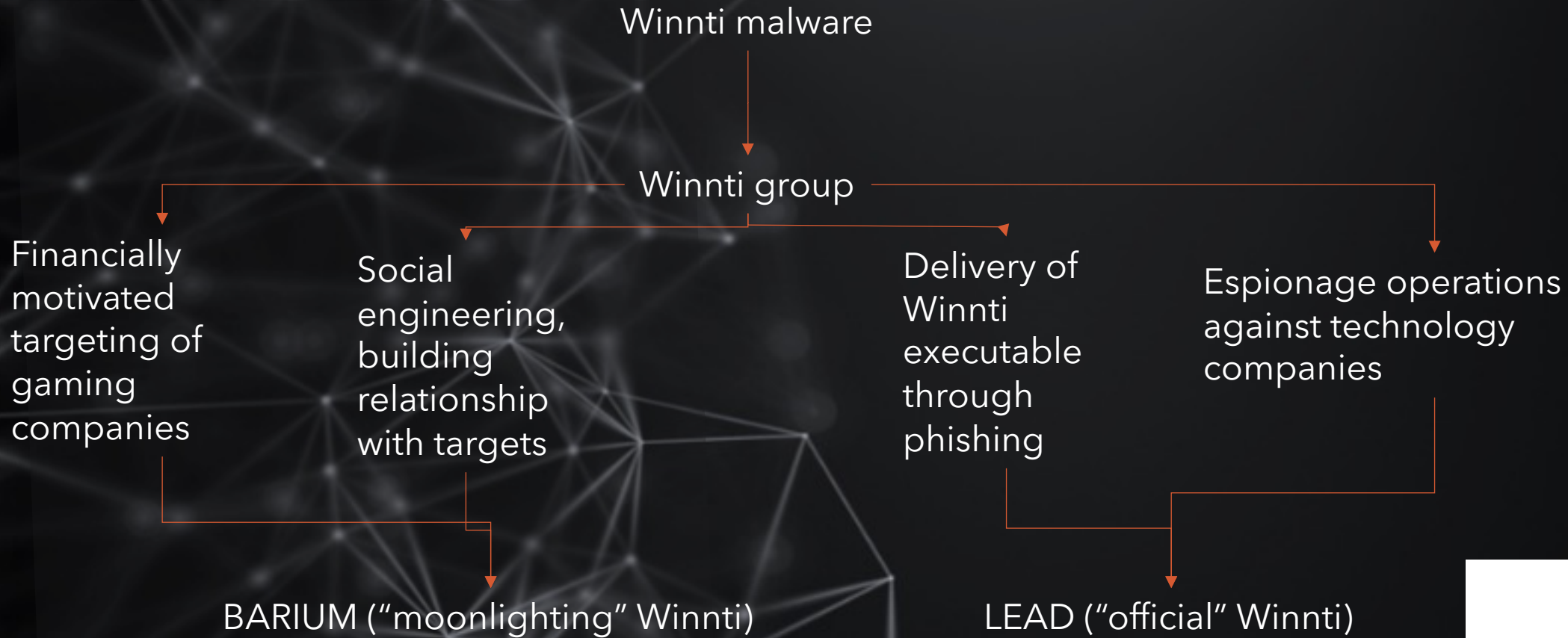
# Winnti - timeline

- In 2017 Microsoft announces that it tracks Winnti as two distinct groups – BARIUM and LEAD.
- BARIUM: Targets gaming, multimedia, Internet content creators.
- LEAD: Industrial espionage.

## Winnti activity groups: BARIUM and LEAD

Microsoft Threat Intelligence associates Winnti with multiple *activity groups*—collections of malware, supporting infrastructure, online personas, victimology, and other attack artifacts that the Microsoft intelligent security graph uses to categorize and attribute threat activity. Microsoft labels activity groups using code names derived from elements in the periodic table. In the case of this malware, the activity groups strongly associated with Winnti are BARIUM and LEAD. But even though they share the use of Winnti, the BARIUM and LEAD activity groups are involved in very different intrusion scenarios.

# Winnti - timeline



# Winnti - timeline

- In 2017 TrendMicro describes how Winnti abuses GitHub for C2.
- Describes Winnti as a threat actor linked to cybercrime.
- Mentions PlugX as a major malware in Winnti arsenal.
- Link: New version of Winnti backdoor BKDR64\_WINNTI.ONM.

## Winnti Abuses GitHub for C&C Communications

The Winnti group, a threat actor with a past of traditional cybercrime — particularly with financial fraud, has been seen abusing GitHub by turning it into a conduit for the C&C communications of their seemingly new backdoor.

### *Following Winnti's Trails*

The GitHub account used by the threat actor was created in May 2016. It created one legitimate project/repository (*mobile-phone-project*) in June 2016, derived from another generic GitHub page.

The repository for Winnti's C&C communications was created on August 2016. We surmise that the GitHub account was not compromised, and instead created by Winnti. By March 2017, the repository already contained 14 different HTML pages created at various times.

# Winnti - timeline

- Also in 2017 TrendMicro publishes a research again treating whole spectrum of activity as a single entity.
- Link: “unreported malware samples that we attributed to the group based on the malware arsenal” -> infrastructure, domain registration.

## APT & Targeted Attacks

# Examining a Possible Member of the Winnti Group

We take a closer look at an individual who we believe might be connected to the Winnti group and provide better insights into some of the tools — notably the server infrastructures — as well as the scale in which they operate.

By: Trend Micro  
April 19, 2017  
Read time: 5 min (1436 words)

## Who is the Winnti group?

The group behind the Winnti malware (which we will call the Winnti group for brevity) sprung up as a band of traditional cyber crooks, comprising black hats whose technical skills were employed to perpetrate financial fraud. Based on the use of domain names they registered, the group started out in the **business of fake/rogue anti-virus products** in 2007. In 2009, the Winnti group shifted to targeting gaming companies in South Korea using a self-named data- and file-stealing malware.

Winn

- Also publ again spec sing
- Link malv attrik base arse dom

关于66云

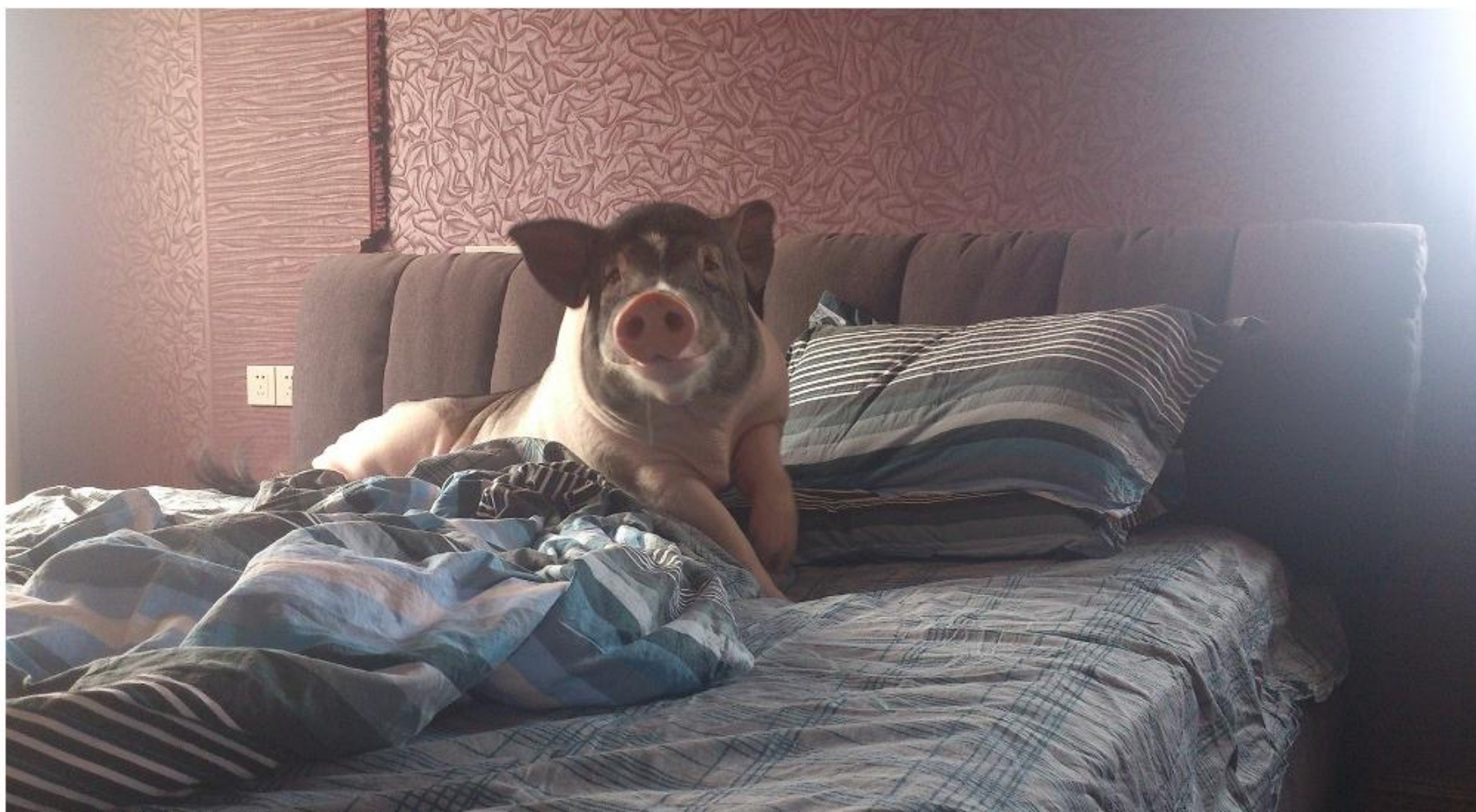
66云是全国首家采用 Azure Pack 私有云架构体系的服务商, 通过使用 Windows Azure 技术, 可以提供与公共 Windows Azure 体验相一致的丰富的自助式多租户云。用户只需简单部署, 就可以以较低成本运行多种不同类型的工作负载。

现已开通香港, 日本, 韩国, 美国, 欧洲区域。

[自助购买 操作手册。](#)

联系

Mail: [Admin#66.To\(#改为@\)](#)



e of the

band of  
nancial

nies in

# Winnti - timeline

---

- 401 Threat Research Group published few pieces in 2017 and the summary Burning Umbrella report.
- Linking of large number of operations to the Winnti cluster – “Winnti umbrella”.
- High confidence in attribution.

## Burning Umbrella

An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers.

---

1. The Chinese intelligence apparatus has been reported on under many names, including Winnti, PassCV, APT17, Axiom, LEAD, BARIUM, Wicked Panda, and GREF.
2. The overlap of TTPs and infrastructure between the Winnti umbrella and other groups indicates the use of shared human and technology resources working towards an overarching goal. Operational security mistakes allow the linking of attacks on lower value targets to higher value campaigns. Reuse of older attack infrastructure, links to personal networks, and observed TTPs play a role in this overlap.

# Winnti - timeline

- In 2018 US DoJ publishes indictment against MSS officers.
- "Members of the conspiracy targeted, among other things, companies in the aerospace and other high-technology industries, and attempted to steal intellectual property and confidential business information, including information that was commercial in nature"

FOR IMMEDIATE RELEASE

Tuesday, October 30, 2018

## **Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years**

Chinese intelligence officers and those working under their direction, which included hackers and co-opted company insiders, conducted or otherwise enabled repeated intrusions into private companies' computer systems in the United States and abroad for over five years. The conspirators' ultimate goal was to steal, among other data, intellectual property and confidential business information, including information related to a turbofan engine used in commercial airliners.

On or before May 24, 2012, a member of the conspiracy installed Winnti malware in Capstone Turbine's computer systems, and the malware, as programmed, sent "beacons" to domain names hosted by DNS ACCOUNT-1, as well as to a blog controlled by "mer4en7y," which is an alias used by GAO. Malware is designed to "beacon" in order to, among other things, notify members of the conspiracy that the malware has been successfully installed.

# Winnti - timeline

- In 2019 Chronicle published research on Linux variant of Winnti malware.
- Identified during intrusion analysis in the environemnet of Vietnamese gaming company.
- Intrusion dated back to 2015.

## Winnti: More than just Windows and Gates



Chronicle · Follow

Published in Chronicle Blog · 7 min read · May 15, 2019

### Technical Analysis

The Linux version of Winnti is comprised of two files: a main backdoor (libxselenium) and a library (libxselenium.so) used to hide it's activity on an infected system.

As with other versions of Winnti, the core component of the malware doesn't natively provide the operators with distinct functionality<sup>8</sup>. This component is primarily designed to handle communications and the deployment of modules directly from the command-and-control servers. During our analysis, we were unable to recover any active plugins. However, prior reporting<sup>9</sup> suggests that the operators commonly deploy plugins for remote command execution, file exfiltration, and socks5 proxying on the infected host. We expect similar functionality to be leveraged via additional modules for Linux.

## Winnti - timeline

- In 2019 ESET publishes summary of Winnti activity, concluding that it is part of same activity cluster like Axiom, Barium, APT41...
- Link: malware, supply chain attacks.

## CONNECTING THE DOTS

### Exposing the arsenal and methods of the Winnti Group

Marc-Etienne M.Léveillé  
Mathieu Tartare

#### Key Findings

- One of the goals of the group, or its subgroups, is cryptocurrency mining. The Winnti Group has deployed cryptocurrency mining software using the backdoor they added in *games and software in 2018*.
- There are strong links in the tools and the techniques used in multiple major supply-chain attacks in past years. These links indicate that the following incidents were likely performed by the same group: *CCleaner*, *NetSarang*, *Asus* and *games and software in 2018*.
- This report documents a previously unanalyzed backdoor used by the Winnti Group. Called *PortReuse* by its authors, this Windows backdoor is a passive network implant that injects itself into a process that is already listening on a network port and waits for an incoming magic packet to trigger the malicious code.

**Winnti Group:** For ESET researchers, this is the group that performed the attacks on multiple organizations using the tools and techniques described in this paper, regardless of their intent. Whether they are part of a single group or multiple subgroups is of less importance. The relationships that can be drawn around their different attacks is sufficient to show they were at least in contact.

# Winnti - timeline

- In 2019 Mandiant published report on APT41 „Double Dragon” operation emphasizing the split between espionage and financially motivated activity.

APT41 uses many of the same tools and compromised digital certificates that have been leveraged by other Chinese espionage operators. Initial reports about HIGHNOON and its variants (reported publicly as "Winnti") dating back to at least 2013 indicated the tool was exclusive to a single group, contributing to significant conflation across multiple distinct espionage operations.

- APT41 overlaps at least partially with public reporting on groups including BARIUM (**Microsoft**) and Winnti (**Kaspersky**, **ESET**, **Clearsky**). In some cases, the primary observed similarity in the publicly reported **Winnti** activity was the use of the same malware—including HIGHNOON—across otherwise separate clusters of activity.

## Certificate Overlap

A digital certificate issued by YNK Japan that was publicly reported as being used by Winnti has been used by multiple Chinese espionage operators, including APT17, and APT20, and APT41.

Issuer: CN=VeriSign Class 3 Code Signing 2009-2 CA

Subject: CN=YNK JAPAN Inc

Serial Number: 67:24:34:0d:db:c7:25:2f:7f:b7:14:b8:12:a5:c0:4d

Issue-Date: 11/27/09 , Expiration-Date: 11/27/11

# Winnti - timeline

## Financially motivated campaigns

Unlike other observed Chinese espionage operators, APT41 conducts explicit financially motivated activity, which has included the use of tools that are otherwise exclusively used in campaigns supporting state interests.

## Espionage operations

Targeting is consistent with China's national strategies to move production capabilities upmarket into research and development (R&D)-heavy fields. These initiatives were especially highlighted with "Made in China 2025,"

POISONPLUG  
POISONPLUG.SHADOW

hrsimon59@gmail.com

APT41



# Winnti - timeline

- In 2020 US DoJ once again publishes an indictment related to Winnti.
- DoJ grouped various monikers as well, though notably omitting the LEAD.

FOR IMMEDIATE RELEASE

Wednesday, September 16, 2020

## **Seven International Cyber Defendants, Including “Apt41” Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally**

**Two Defendants Arrested in Malaysia; Remaining Five Defendants, One of Whom Allegedly Boasted of Connections to the Chinese Ministry of State Security, are Fugitives in China**

In August 2019 and August 2020, a federal grand jury in Washington, D.C., returned two separate indictments charging five computer hackers, all of whom were residents and nationals of the People’s Republic of China (PRC), with computer intrusions affecting over 100 victim companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media

11. Since at least 2012, JIANG and QIAN have been collaborating together. Since that time, QIAN and JIANG have conducted criminal computer hacking activity, together and with others known and unknown to the Grand Jury, which has in some instances been tracked by cybersecurity professionals under the threat group labels “APT41,” “Barium,” “Winnti,” “Wicked Panda,” and “Wicked Spider.” QIAN and JIANG have also collaborated with, and used overlapping tactics, techniques, procedures, and malware with, other computer hackers, including Zhang Haoran and Tan Dailin, whose activities have been tracked under those same threat group labels. QIAN, JIANG, and those other computer hackers carried out their hacking using specialized malware, such as malware that cybersecurity experts named “PlugX/Fast,” “Winnti/Pasteboy,” “Shadowpad,” “Barlaiy/Poison Plug,” and “Crosswalk/ProxIP.”

# Winnti - timeline

- In 2020 we published research on the newly discovered samples of Winnti malware targeting a gaming company and a chemical company.
- More relationship to LEAD branch.
- Linked through malware. Similarities in code and functionality.

## WINNTI GROUP: Insights From the Past

Apr 20, 2020 | Blog

**Newly uncovered DNS tunnelling technique, and new campaign against South Korean gaming company**

### Executive Summary

- In January 2020, [QuoIntelligence](#) (QuoINT) detected a new Winnti sample uploaded to a public virus scanner from a German location. Following our preliminary analysis, we assessed with high confidence that the sample was used to target a previously unreported German chemical company. As part of our responsible disclosure, we alerted the affected entity, the local Law Enforcements, and our clients.

## Winnti - timeline

- In 2020 FireEye reported on APT41 espionage operation exploiting Citrix NetScaler, Cisco routers, Zoho ManageEngine.
- Use of Cobalt Strike and Meterpreter.

### This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits

CHRISTOPHER GLYER, DAN PEREZ, SARAH JONES, STEVE MILLER

MAR 25, 2020 | 12 MIN READ | LAST UPDATED: NOV 08, 2021

It is notable that we have only seen these exploitation attempts leverage publicly available malware such as Cobalt Strike and Meterpreter. While these backdoors are full featured, in previous incidents APT41 has waited to deploy more advanced malware until they have fully understood where they were and carried out some initial reconnaissance. In 2020, APT41 continues to be one of the most prolific threats that FireEye currently tracks. This new activity from this group shows how resourceful and how quickly they can leverage newly disclosed vulnerabilities to their advantage.

# Winnti - timeline

- In 2022 Cybereason describes suite of tooling used by Winnti after investigation into industrial espionage operations. - "undetected since at least 2019 with the goal of stealing sensitive proprietary information from technology and manufacturing companies, mainly in East Asia, Western Europe, and North America."
- Moderate-high confidence in attribution to Winnti.
- Linked through malware and TTPs.

## Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques

WRITTEN BY Cybereason Nocturnus

May 4, 2022 | 11 minute read

In 2021, the Cybereason Nocturnus Incident Response Team investigated multiple intrusions targeting technology and manufacturing companies located in Asia, Europe and North America. Based on the findings of our investigation, it appears that the goal behind these intrusions was to steal sensitive intellectual property for cyber espionage purposes.

Cybereason assesses with moderate-high confidence that the threat actor behind the intrusion is the Winnti Group (also tracked as APT41, Blackfly and BARIUM), one of the most

## Winnti - timeline

- In 2022 Group-IB reported on worldwide campaign of APT41.
- Researchers grouped together other monikers including BARIUM and LEAD.
- SQL injections, Cobalt Strike, CertUtil, custom SSL certificates.

## APT41 World Tour 2021 on a tight schedule

4 malicious campaigns, 13 confirmed victims, and a new wave of Cobalt Strike infections

- A state-sponsored group whose goals include cyber espionage and financial gain
- Active since at least 2007
- Also known as BARIUM, Winnti, LEAD, WICKED SPIDER, WICKED PANDA, Blackfly, Suckfly, Winnti Umbrella, Double Dragon
- Some of the group's members were indicted by the US Department of Justice in 2020; **charges** against them include unauthorized access to protected computers, aggravated identity theft, money laundering, and wire fraud

# Winnti - timeline

- Department of Health and Human Services briefing from September 2022 clusters Winnti, Barium, APT41.
- Targeting healthcare since 2014.
- Underscores link to Five-Year plan.



- Chinese State-Sponsored Threat Actor
- Members of APT41 have been actively tracked since 2012
- Also Known As: Double Dragon, Barium, Winnti, Wicked Panda, Wicked Spider, TG-2633, Bronze Atlas, Red Kelpie
- Has been tracked as two separate groups; dependent on operation
- History of targeting healthcare, high-tech, telecommunications, higher education, video games, travel, and news organizations

**WHO IS THIS**



**WINNTI HACKER?**

imgflip.com





Recon

Weaponization

Delivery

Exploitation

Installation

C2

Actions on Objectives

You are somewhere here

**HOW CAN WE DEFINE THIS WINNTI GROUP**

**SO THAT IT CAN BE USEFUL  
FOR OUR SECURITY ORGANIZATION**

# Analytical models to the rescue!

---

- How did you come across Winnti operations?
- Which aspects do you care about most?
- Would you care if attribution was inaccurate?
- How are you using the reporting?

# Analytical models to the rescue!

---

- Instead of dwelling on the clustering specifics create an analytical model that fits your needs and use that.
- Do you really need to track Winnti?
- Why?
- What was the requirement?
- How it will impact your defense posture?

# Making your own Winnti group.

---

- Solution – make your own Winnti!
- Account for:
  - Intent
  - Opportunity
  - Capability
- Why are you following the related reporting?
  - Do you care about targets?
  - Are you worried about alleged supply chain attacks?
  - Proliferation of malware among various groups directs you towards detection of new strains?

# Making your own Winnti group.

- Winnti:

- Targets gaming, multimedia, internet content companies (BARIUM flavor); engineering, manufacturing, pharmaceutical, academia (LEAD flavor).
- Use of Winnti malware. Abuse of stolen digital certificates. Supply chain attacks.
  - BARIUM: social engineering, office macros, LNK files.
  - LEAD: Email delivery of Winnti installation package.
- Use of DDNS, Let's Encrypt, GitHub for C2, infrastructure registration patterns...

# Making your own Winnti group.

Financially motivated adversaries

Foreign intelligence operation

Stolen code certificates

Winnti malware

Cobalt Strike

DNS Tunneling

Cryptomining

Spear-phishing

campaigns

targeting HR,

hiring managers, IT

staff, infosec staff

Your\_Winnti

Tibetan and Chinese journalists, Uyghur and Tibetan activists

Gaming companies

High tech industry

„Hak520“ domain family

GitHub for C2 communication

Let's encrypt certificates

WHOAMI naming convention

DDNS

# Making your own Winnti group.

Financially motivated adversaries

Foreign intelligence operation

Stolen code certificates

Winnti malware

Cobalt Strike

DNS Tunneling

Cryptomining

Spear-phishing

campaigns

targeting HR,

hiring managers, IT

staff, infosec staff

Your\_Winnti

„Hak520“ domain family

GitHub for C2 communication

Let's encrypt certificates

WHOAMI naming convention

DDNS

Tibetan and Chinese journalists, Uyghur and Tibetan activists

Gaming companies

High tech industry

# References

- <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/10/02153102/winnti-more-than-just-a-game-130410.pdf>
- [https://www.trendmicro.com/en\\_us/research/17/d/pigs-malware-examining-possible-member-winnti-group.html](https://www.trendmicro.com/en_us/research/17/d/pigs-malware-examining-possible-member-winnti-group.html)
- <https://securelist.com/games-are-over/70991/>
- <https://securelist.com/winnti-more-than-just-a-game/37029/>
- [https://cyber-peace.org/wp-content/uploads/2018/07/20180503\\_Burning\\_Umbrella.pdf](https://cyber-peace.org/wp-content/uploads/2018/07/20180503_Burning_Umbrella.pdf)
- <https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal>
- <https://www.mandiant.com/resources/reports/supply-chain-analysis-quartermaster-sunshop>
- <https://blogs.blackberry.com/en/2016/10/digitally-signed-malware-targeting-gaming-companies>
- <https://www.justice.gov/opa/press-release/file/1106491/download>
- [https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET\\_Winnti.pdf](https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf)
- <https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/>
- <https://www.cybereason.com/blog/operation-cuckoo-bees-deep-dive-into-stealthy-winnti-techniques>
- <http://web.archive.org/web/20221013072210/https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/>
- <https://www.group-ib.com/blog/apt41-world-tour-2021/>
- <https://www.mandiant.com/resources/reports/apt41-double-dragon-dual-espionage-and-cyber-crime-operation>
- <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer>
- [https://web.archive.org/web/20141107205408/http://www.novetta.com/files/9714/1446/8199/Executive\\_Summary-Final\\_1.pdf](https://web.archive.org/web/20141107205408/http://www.novetta.com/files/9714/1446/8199/Executive_Summary-Final_1.pdf)
- <https://web.archive.org/web/20221206192812/https://www.novetta.com/2015/04/operation-smr-winnti-update/>
- <https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/>
- <https://www.mandiant.com/resources/blog/apt41-initiates-global-intrusion-campaign-using-multiple-exploits>
- <https://www.hhs.gov/sites/default/files/apt41-recent-activity.pdf>
- <https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a>

**Thank you for your time!**

---

Questions?