

CYBERUS

TECHNOLOGY

Botconf 2022

How to Eavesdrop on Winnti in a
Live Environment Using
Virtual Machine Introspection (VMI)

Philipp Barthel & Sebastian Eydam

- Motivation
 - use our VMI tool Tycho to showcase functionality
 - tackle a well known and successful malware



T Y C H O

- Motivation
 - use our VMI tool Tycho to showcase functionality
 - tackle a well known and successful malware
 - Winnti is an APT RAT that has attacked many DAX corporations



T Y C H O

- Motivation
 - use our VMI tool Tycho to showcase functionality
 - tackle a well known and successful malware
 - Winnti is an APT RAT that has attacked many DAX corporations
- Goal
 - detect an infection
 - eavesdrop on the malware
 - ... without being seen



T Y C H O

- Motivation
 - use our VMI tool Tycho to showcase functionality
 - tackle a well known and successful malware
 - Winnti is an APT RAT that has attacked many DAX corporations
- Goal
 - detect an infection
 - eavesdrop on the malware
 - ... without being seen



T Y C H O

↔ The Winnti Detective

About us

Virtual Machine Introspection

About Winnti

The Winnti Detective

- Cyberus
 - founded 2017
 - about 25 employees
 - specialized in virtualization technology and secure workstations
 - involved in discovery of Meltdown and Spectre

- Cyberus
 - founded 2017
 - about 25 employees
 - specialized in virtualization technology and secure workstations
 - involved in discovery of Meltdown and Spectre
- Philipp Barthel
 - student employee studying Cybercrime/Cybersecurity with focus on malware
 - worked 6 months on Winnti analysis
- Sebastian Eydam
 - student employee at the time, now full-time at Cyberus
 - just finished his thesis project about side channel attack mitigations in hypervisors
- Sebastian Manns
- Werner Haas

- **Intrusion Detection System (IDS)**
 - collects sensor information from different sources
 - detects malware signatures, and/or
 - identifies abnormal behaviour

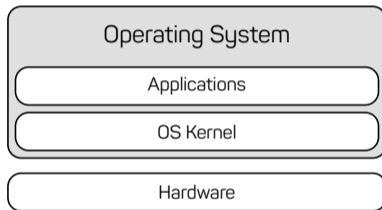
- **Intrusion Detection System (IDS)**

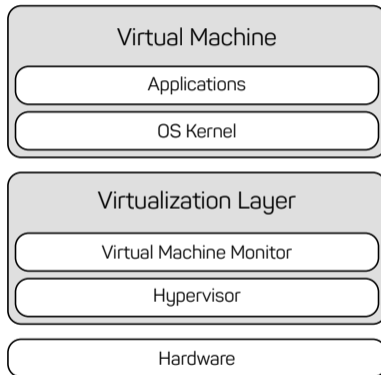
- collects sensor information from different sources
- detects malware signatures, and/or
- identifies abnormal behaviour

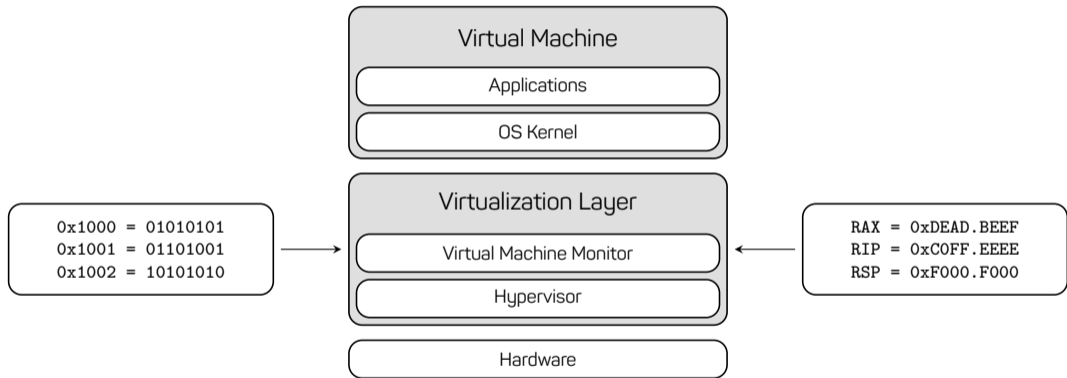
- Trade-off between resistance and visibility:

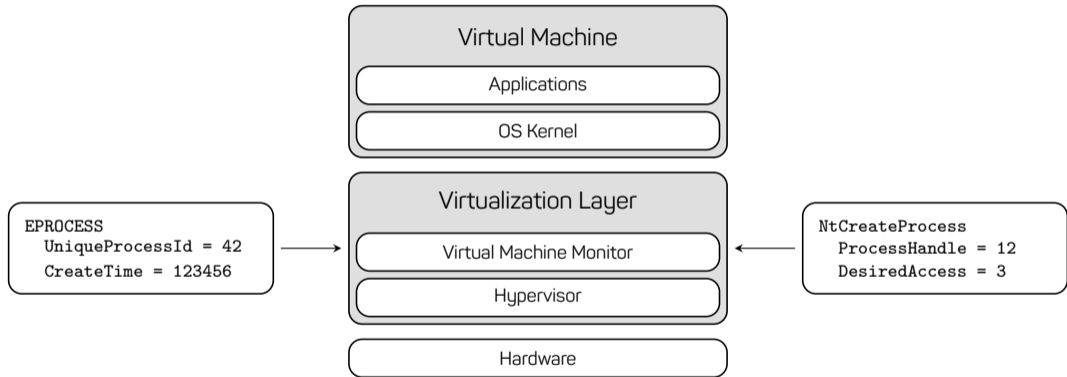
- Host-based IDS (HIDS) - resides on the same system it is designed to protect
- Network-based IDS (NIDS) - relocates the detection mechanism to a different entity

- **Intrusion Detection System (IDS)**
 - collects sensor information from different sources
 - detects malware signatures, and/or
 - identifies abnormal behaviour
- Trade-off between resistance and visibility:
 - Host-based IDS (HIDS) - resides on the same system it is designed to protect
 - Network-based IDS (NIDS) - relocates the detection mechanism to a different entity
- VMI leverages virtualization achieve HIDS visibility and NIDS resistance









Victim PC



Analyst PC

- attach to processes (`calc = tycho.open_process("calc.exe")`)

- attach to processes (`calc = tycho.open_process("calc.exe")`)
- manipulate processes (`calc.pause()`)
- inspect processes (`calc.read_linear(0, 1024)`)

- attach to processes (`calc = tycho.open_process("calc.exe")`)
- manipulate processes (`calc.pause()`)
- inspect processes (`calc.read_linear(0, 1024)`)
- syscall breakpoints (`add_syscall_whitelist(syscalls.NtCreateFile)`)
- interpret syscalls

- group of hackers
- presumably a state-sponsored Chinese thread actor
- deploy a RAT called Winnti

The Winnti Group, active since at least 2012, is responsible for high-profile supply-chain attacks against the software industry, leading to the distribution of trojanized software (such as CCleaner, ASUS LiveUpdate and multiple video games) that is then used to compromise more victims. Recently, ESET researchers also discovered a campaign of the Winnti Group targeting several Hong Kong universities with ShadowPad and Winnti malware.

Source: <https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/>

- Winnti is still going strong today...

Targeted companies



Gaming: Gameforge, Valve



Software: Teamviewer



Technology: Siemens, Sumitomo, Thyssenkrupp



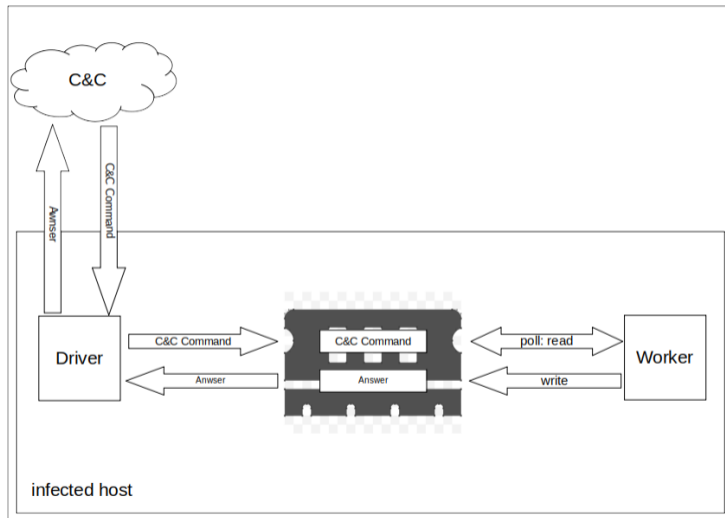
Pharma: Bayer, Roche



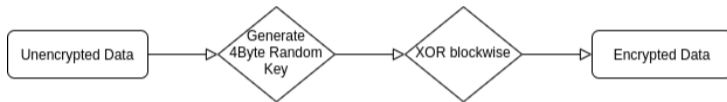
Chemical: BASF, Covestro, Shin-Etsu

Source: <https://interaktiv.br.de/winnti/english/>

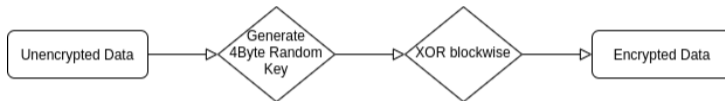
- “Any DAX corporation that hasn’t been attacked by Winnti must have done something wrong.”
- an IT security expert quoted by German public television.
- at least 35 infected companies until 2018 according to Kaspersky Lab



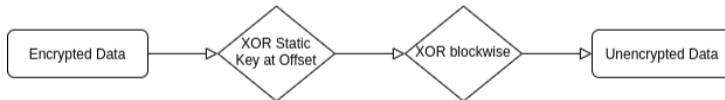
- Encryption



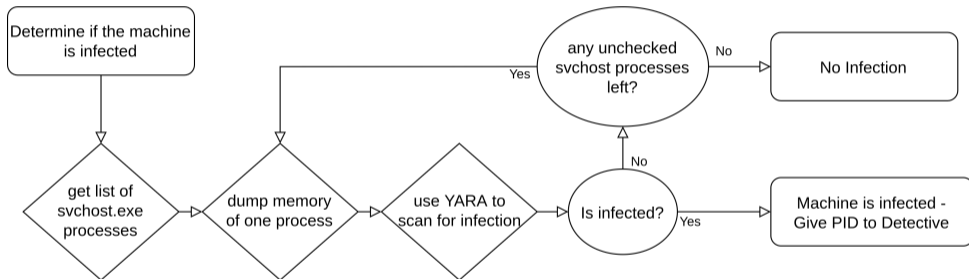
- Encryption



- Decryption




- **Detector** - detects infected svchost if applicable
- **Detective** - differentiates genuine svchost functionality / malicious Winnti usage
 - extracts data read/written by the Worker Component
- **Decryptor** - decrypts the found data



- inspects all ntDeviceIoControlFile system calls of the given process
- scans for Winnti's custom IOCTL codes
 - genuine functionality
 - malicious functionality
 - 0x156003 write
 - 0x15E007 read
- reads encrypted communication data from system call parameters

- Thyssenkrupp Script to scan for infections was used
- replayattack via TCP to send Helo (sic!) and GetQueryHostInformation Packets
- doublecheck using Wireshark - Can we extract what has been sent?



TKCERT / winnti-nmap-script Public

<> Code Issues Pull requests Actions Projects Wiki Security

master 1 branch 0 tags Go to file Code

sruester Changed l2 to random value fcc7859 on May 22, 2018 4 commits	
LICENSE	Initial commit 4 years ago
README.md	Added installation section to README 4 years ago
winnti-detect.nse	Changed l2 to random value 4 years ago

README.md

Nmap Script to scan for Winnti infections

This Nmap script can be used to scan hosts for Winnti infections. It uses parts of Winnti's protocol as seen in the wild in 2016/2017 to check for infection and gather additional information.

Source: <https://github.com/TKCERT/winnti-nmap-script>

Nmap Script to scan for Winnti infections

This Nmap script can be used to scan hosts for Winnti infections. It uses parts of Winnti's protocol as seen in the wild in 2016/2017 to check for infection and gather additional information.

Winnti

Winnti is a malware that is used by some APT groups.

It has been used since at least 2013 and has evolved over time. You can find some information here

- <https://kasperskycontenthub.com/wp-content/uploads/sites/43/vpdfs/winnti-more-than-just-a-game-130410.pdf>
- https://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf
- <https://hitcon.org/2016/pacific/0composition/pdf/1201/1201%20R2%201610%20winnti%20polymorphism.pdf>

SecOps Warning

WINNTI ONLY SUPPORTS ONE CONNECTION AT A TIME. IF YOU SCAN A HOST FOR WINNTI YOU WILL RESET THE CURRENT CONNECTION IF THERE IS ONE.

Let's take a look at the demovideo

- Virtual Machine Introspection
 - non-invasive monitoring capabilities
 - live analysis of running Malware
- Winnti
 - notorious hacker group and RAT tool
 - well-studied Malware, ideal for experimentation
- Tycho-based analysis
 - YARA rule to detect infected process
 - thysenkrupp's nmap script as C2 emulator
 - ntDeviceIOControlFile-hooking to observe communication
- philipp.barthel@cyberus-technology.de
- sebastian.eydam@cyberus-technology.de