Decade of the RATs

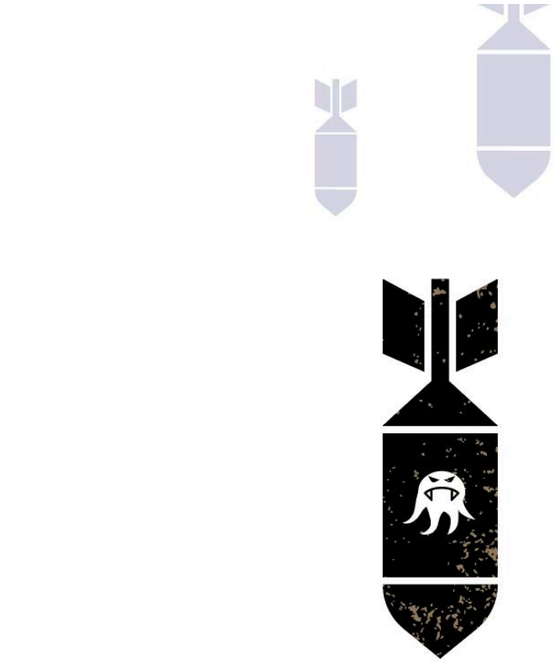
Custom Chinese Linux Rootkits for Everyone

Kevin Livelli, Director of Threat Intelligence, BlackBerry

Fine Print

Legal Disclaimer

The information contained in this presentation is intended for educational purposes only. BlackBerry does not guarantee or take responsibility for the accuracy, completeness and reliability of any third-party statements or research referenced herein. The analysis expressed in this report reflects the current understanding of available information by our research analysts and may be subject to change as additional information is made known to us. Audiences are responsible for exercising their own due diligence when applying this information to their private and professional lives. BlackBerry does not condone any malicious use or misuse of information presented in this presentation.



Acknowledgements

Black Hat Review Board

BlackBerry Executive Leadership + Anthony Freed

Jon Miller, Ryan Smith, Tom Wabiszczewicz

Jeff Tang + Applied Research Team

Researcher X

WHO IS

KEVIN LIVELLI

Current:

- Director of Threat Intelligence, BlackBerry

Prior:

- Investigative journalist, CBS News 60 MINUTES
- Supervising Investigator, NYC Civilian Complaint Review Board

- - - - - -

twitter.com/kevinlivelli
linkedin.com/in/kevinlivelli

FORMAT

“30 MINUTES”

Questions….and Answers

TAKEAWAYS:

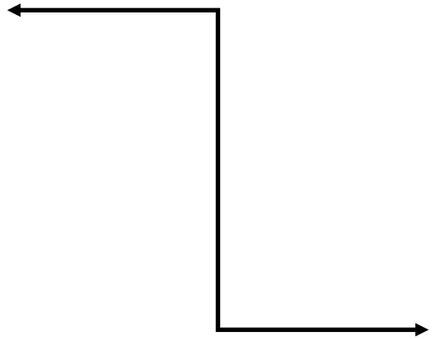
- Critical approaches to malware analysis
- How to question your own findings
- How to question your own thinking

What did we find?

ANSWER:

FULL STACK OF LINUX MALWARE + SPLINTER CELL

“WINNTI”



1. WINNTI GROUP
2. PASSCV
3. BRONZE UNION (APT27, EMISSARY PANDA)
4. CASPER (LEAD)
5. (WNLXSPLINTER)

ANSWER:

LINUX SPLINTER CELL TOOLSET WINNTILNX **:**

1. Interactive installer script
2. Build environments (2) – remote and local
3. Backdoors (3 variants) – designed to run with rootkits
4. Rootkits (2 variants) -- LKM
5. Control panel – with GUI, Linux and Windows
6. Botnet - Linux XOR.DDoS

ANSWER:

LINUX SPLINTER CELL TOOLSET C2 STAND-OUTS**:**

10.x IPs -> C2 inside the target environment

Extensive abuse of legitimate cloud service providers

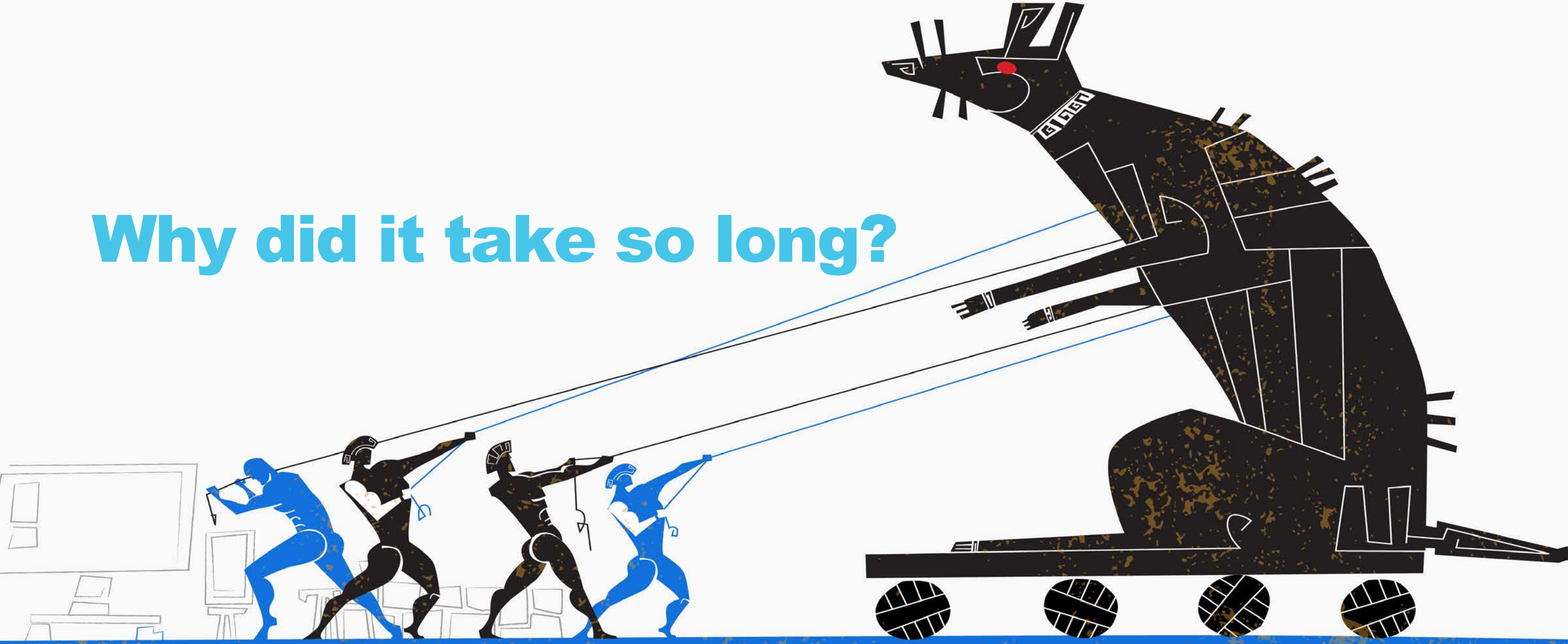
ANSWER:

SAME APTs, DIFFERENT PLATFORMS:

ANDROID: 2 new implants (PASSCV, LEAD/CASPER)

WINDOWS: 4 new variants of ZxShell droppers

Why did it take so long?



WRONG ANSWERS:

NOT ENOUGH RELEVANT "*APT GROUP HERE*" RESEARCH

NOT ENOUGH PRODUCT / SERVICES COVERAGE

POSSIBLE ANSWERS:

LINUX IS IGNORED BY VIPs AT TARGET ORGANIZATIONS

LINUX IS IGNORED BY INFOSEC VENDORS

LINUX IS ASSUMED TO BE MORE SECURE

WE FORGOT THAT EVERTHING OLD EVENTUALLY COMES FULL CIRCLE

CUSTOM LKM ROOTKITS

PWNLINX4 (original):

- Code appears to have been lifted directly from Ivan Skylarov's *Programming Linux Hacker Tools Uncovered: Exploits, Backdoors, Scanners, Sniffers, Brute-Forcers, Rootkits* (2007)

PWNLINX6 (updated):

- Code appears to be based on a modified version of the Suterusu Rootkit
- Referred to by attackers as "xinted.ko"
- Compiled with newer version of GCC, with several notable features absent, e.g. routines to directly patch TCP/UDP tables
- Also changed: custom network protocol to replace previously used ioctl codes allowing easier communication between kernel and user side. Led to the discovery of an additional backdoor

INTERACTIVE INSTALLER SCRIPT

```
echo "============================================================"
echo "===      Lancer Remote Online Compilation System v2.0      ==="
echo "============================================================"
echo "current system   = ${ret}bit"
echo "kernel version   = $__kernel"
echo "header version   = $__header"
echo "md5 hash version = $__version"
echo "============================================================"
```

- Compressed bash script - over 400 lines long

- Three additional command line arguments required to execute:
    1. “username”
    2. “build”
    3. “force_mode”

- Checks to see if LKM was already compiled for the current header version
    GET /build/check?args=version|kernel|force_mode&token=*{result from auth request}*

- Self-identifies as “Lancer Remote Online Compilation System v2.0” – suggesting a v1.0

LINUX BUILD ENVIRONMENTS: REMOTE

- Build Environment 1: “/opt/uOnlineBuilder64/core/build/**yang**/rk”
  - /opt/uOnlineBuilder64/core/build/yang/rk/lkm.c
  - /opt/uOnlineBuilder64/core/build/yang/rk/autoipv6.mod.c
  - “”/build/yang/AB1167FF11C7B8642D547D84AEDD8B46/2.6.32-358. el6.x86_64
- Build Environment 2: /opt/uOnlineBuilder64/core/build/**hehe**/rk
  - /opt/uOnlineBuilder64/core/build/hehe/rk/lkm.c
  - /opt/uOnlineBuilder64/core/build/hehe/rk/autoipv6.mod.c
  - “”/build/hehe/4F666C7AA5F592EF64E9B2AFFE2 67B0F/2.6.32-754.6.3.el6.x86_64
- Build Environment 3: /opt/uOnlineBuilder64/core/build/**maomao**/rk
  - /opt/uOnlineBuilder64/core/build/maomao/rk/lkm.c
  - /opt/uOnlineBuilder64/core/build/maomao/rk/ip4tables.mod.c
  - “”/build/maomao/01944A09FD7592DDFEF4AD4825AB6329/2.6.32-431.11.29. el6.ucloud.x86_64

What’s Interesting here:

- ✓ Online and On-the-Fly
- ✓ Delivers the rootkit/backdoor not just by MD5 hash but username as well
- ✓ Check out those usernames!
- ✓ Check out those filenames!

LINUX BUILD ENVIRONMENTS: LOCAL

- Build Environment: /root/Desktop/dns
  - /root/Desktop/dns/lkm.c
  - /root/Desktop/dns/snd_raw.mod.c
  - /usr/src/kernels/2.6.32-642.el6.x86_64

- Build Environment: /var/tmp/.1
  - /var/tmp/.1/lkm.c
  - /var/tmp/.1/autoipv6.mod.c
  - /usr/src/kernels/3.10.0-693.2.2.el7.x86_64

- Build Environment: /var/tmp/Linux_Server
  - /var/tmp/Linux_Server/lkm.c
  - /var/tmp/Linux_Server/dhcp.mod.c
  - /usr/src/kernels/2.6.32-358.14.1.el6.x86_64

- Build Environment: /dev/shm/2.6.32microcode
  - /dev/shm/2.6.32microcode/lkm.c
  - /dev/shm/2.6.32microcode/microcode.mod.c
  - /usr/src/kernels/2.6.32-358.14.1.el6.x86_64

- Build Environment: //home/rhudgins/2.6.32floppy
  - /home/rhudgins/2.6.32floppy/lkm.c
  - /home/rhudgins/2.6.32floppy/ipmi_devintf.mod.c
  - /usr/src/kernels/2.6.32-358.14.1.el6.x86_64

What's Interesting here:

✓ Compiled locally, directly on target machine
✓ Access to the server already achieved
✓ Earliest compile date on rootkit: 2013

WANT MORE CUSTOM CHINESE LINUX ROOTKITS FOR EVERYONE?

Installation script communicates to 1 of 2 hosts:

32-bit = 3232.3389[.]la
64-bit = 6464.3389[.]la

Looks a lot like historic PASSCV domain = 3389[.]hk
Found new hosts:

64.3389[.]hk. ---> 150.242.210[.]181
32.3389[.]hk ---> 150.242.210[.]180

Relatively unique HTTP server: beegoServer:1.6.0 (https://beego.me/)

Is ‘WINNTI’ responsible for the original 2014-2015 Linux XOR.DDoS botnet?

ANSWER:

YES

- ✓ Same targeting of video game industry
- ✓ Same device used for rootkit functionality: “/proc/rs_dev”
- ✓ Same XOR key to obfuscate network traffic: BB2FA36AAA9541F0
- ✓ Same modifications of the open-source Suterusu Rootkit
- ✓ Initial online build servers essentially identical

Look familiar?

Additional Parameter	Value	Function
iid=	CE74BF62ACFE944B2167248DD0674977	Lookup Hash of Kernel
username=	admin	Username to Access Build Server
&password=	admin	Password to Access Build Server
ip=	103.25.9[.]245:8005|103.240.141[.]50:8005[snip]	C2 Servers
&ver=	3.8.0-19-generic\ SMP\ mod_ unload [snip]	Full Kernel Version
kernel=	3.8.0	Base Kernel Version

Is ‘WINNTI’ behind the development of one of the most widely used, commercially available RATs?

ANSWER = ???

PNWDROID4 and NetWire

NetWire – legit
PWNDROID4 – not legit

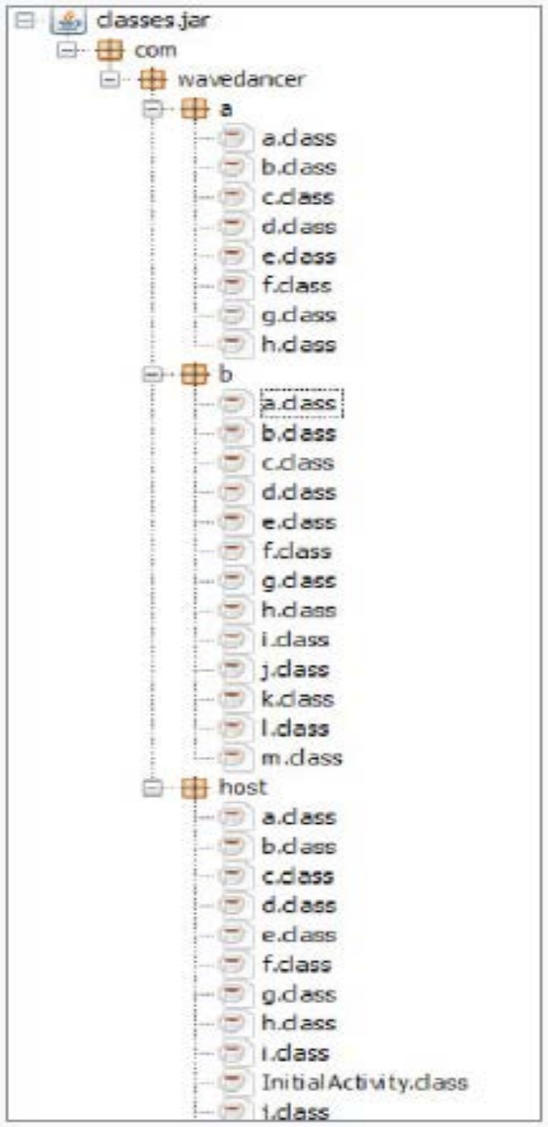
PWNDROID4 APK last modified =
June 16, 2015

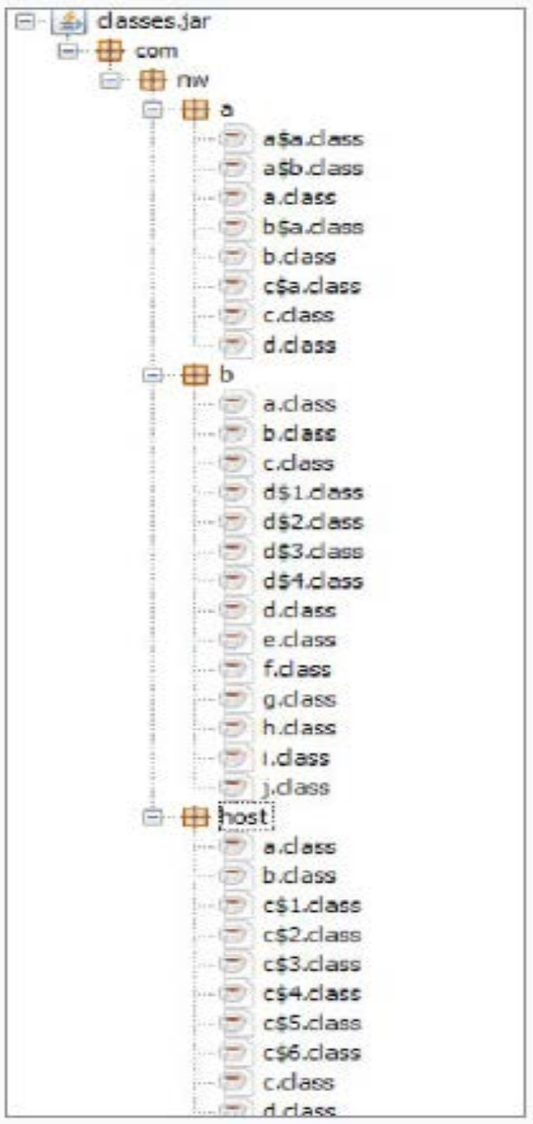
NetWire Android announcement =
January 2, 2017

NetWire final release =
March 23, 2017

Difference in time = 18 mos – 2 yrs

?





Adware? Who Cares?!

ANSWER = NOT MANY PEOPLE

Alert Fatigue

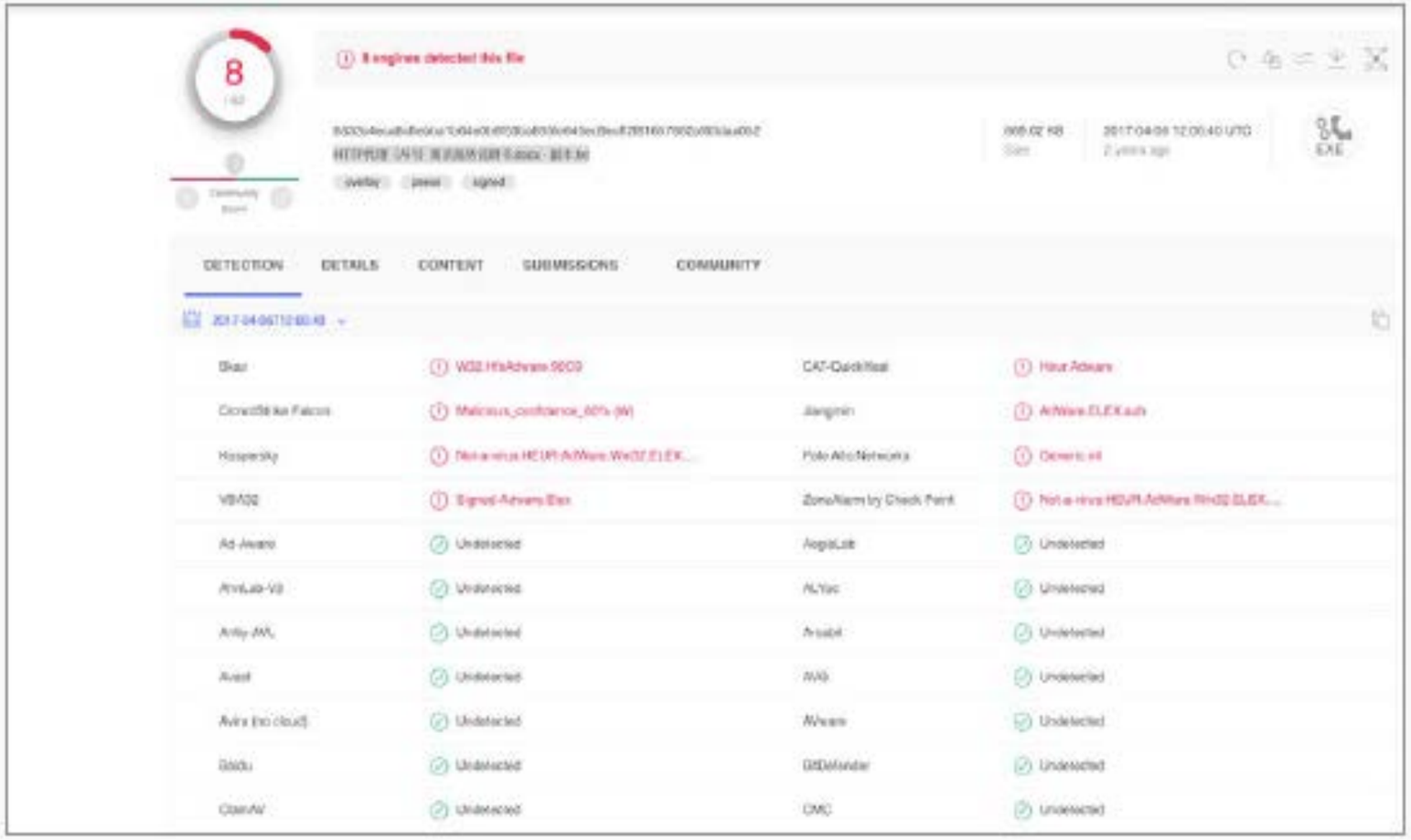
PUP/PUA alerts

Flagged as Adware

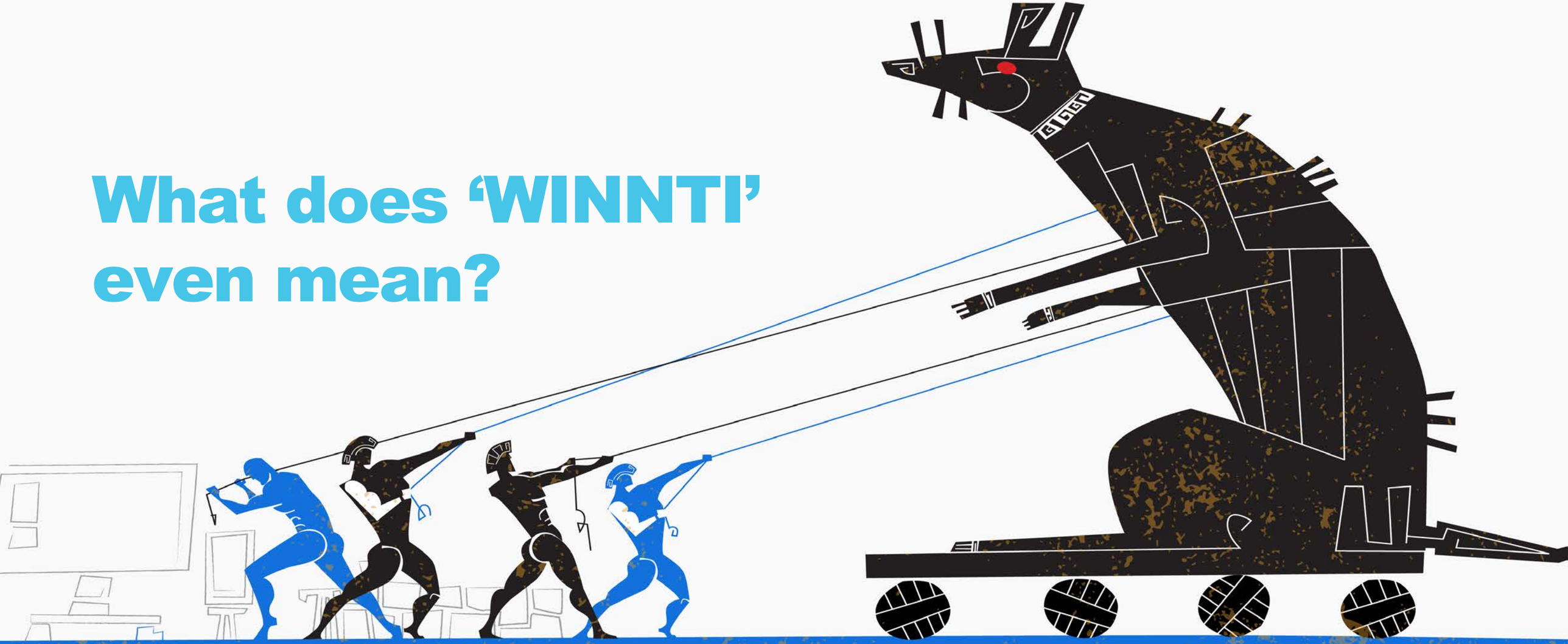
Adware is Boring

Found & Ignored vs.
Found & Investigated

Part of a larger APT trend



What does ‘WINNTI’ even mean?



ANSWER: It's an Approach

"WINNTI" = a **BACKDOOR,** an **ATTACK GROUP**, an "**UMBRELLA**," an **APPROACH**

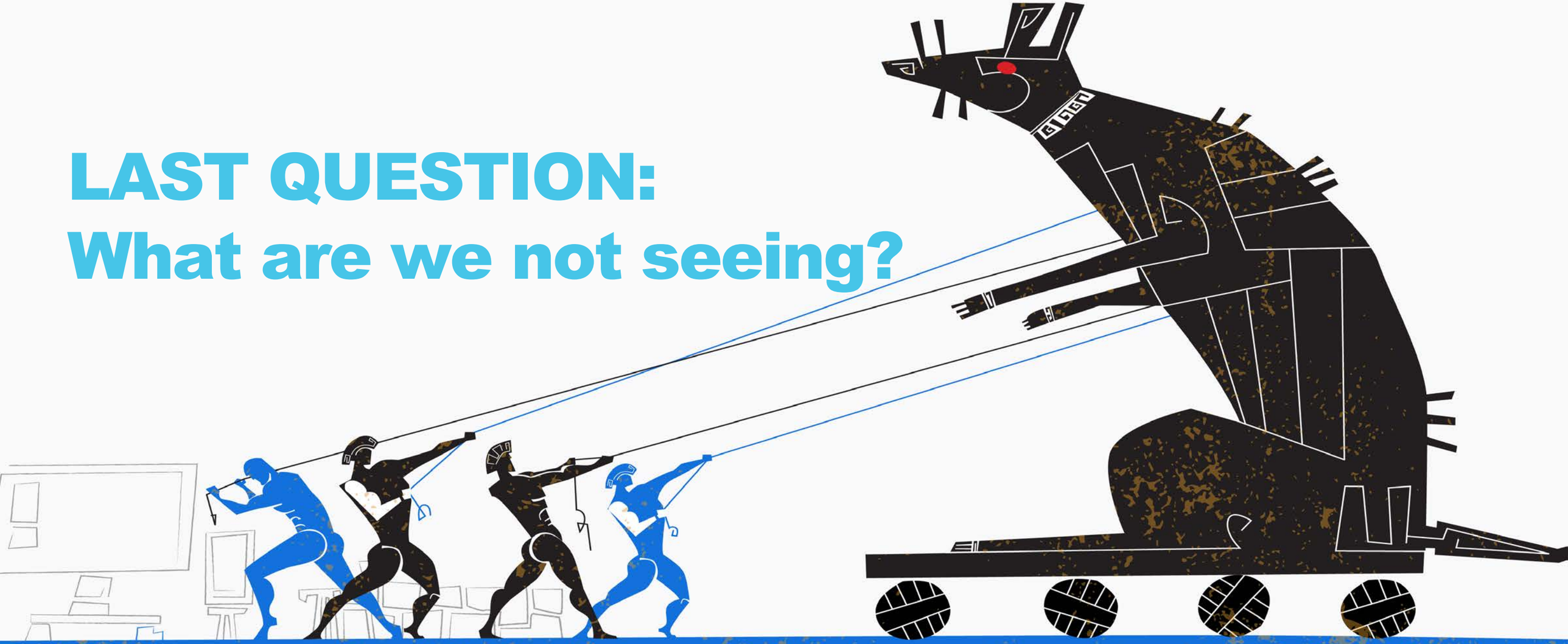
5 Derivative APT Groups assessed to be acting in the interest of the Chinese government:

WINNTI GROUP **PASSCV** **BRONZE UNION / EMISSARY PANDA / APT27**
LEAD / CASPER **(WLNXSPLINTER)** emerging **…..BUT WAIT, THERE'S MORE!**

Commonalities:

- Observed attacking **video game companies** to steal code-signing certificates which they used to sign their malware, as well as attacking the gaming companies for criminal purposes to produce revenue.
- **Share tools and/or C2**, suggesting several possible scenarios: a formal "digital quartermaster" arrangement (a la FireEye); an informal "hacker forum" type of tool swap; personnel overlap between the groups; or a re-tasking of the same groups toward different target sets.
- **Targeting runs the gamut** of nearly all verticals, and activities range from simple cybercrime to full-blown economic espionage, and from internal monitoring of politically dissenting populations to more traditional military and strategic nation state espionage. These groups' collective **palette is wide and well-developed**, touching nearly every industry sector across a huge geographic area.

LAST QUESTION:
What are we not seeing?



THANK YOU

blackberry.com/RATs