HARDWARE VULNERABILITIES AND BIOS/UEFI SECURITY

HARDWARE VULNERABILITIES

MELTDOWN AND SPECTRE
JANUARY 2018
• Variant 1: Bounds Check Bypass – CVE-2017-5753
• Variant 2: Branch Target Injection – CVE-2017-5715
• Variant 3: Rogue Data Cache Load – CVE-2017-5754
• Variant 3a: Rogue System Register Read – CVE-2018-3640
• Variant 4: Speculative Store Bypass – CVE-2018-3639

MELTDOWNPRIME AND SPECTREPRIME
FEBRUARY 2018
SpectrePrime code proposed by researchers as a proof of concept leads to the success of 99.95% of the attacks on an Intel processor (the success rate of the usual attacks by Spectre reaches 97.9%).

GLITCH
MAY 2018
The specialists successfully tested the Glitch technique on an Android device with Chrome and Firefox browsers. They were able to compromise the device in just 2 minutes. To exploit the attack technique, all they had to do was to upload the malicious JavaScript code to the target device.

TLBLEED
JULY 2018
It was demonstrated that cryptographic keys and other important data can be extracted from another running program with a minimum success rate of 98%. Despite the fact that the vulnerability was not identified with CVE, OpenBSD developers decided not to support Hyper-Threading in Intel processors.

99.95%
success rate when using SpectrePrime

2 MINUTES
needed to compromise an Android-based device using the GLitch technique

98%
success rate of the attack and cryptographic keys extraction using TLBleed
BIOS/UEFI THREATS

LOW THREAT ACTIVITY

WinCIH
Mebromi/BIOSkit
Computrace


LOW RESEARCH ACTIVITY

ACPI Rootkit
IceLord Rootkit
BIOS Patching
Rakshasa

PCI OptRom Rootkit
SMM Rootkit

TARGETED ATTACKS

BadBIOS Hysteria
DEITYBOUNCE
HT rloader
BANANABALLOT
DerStarke
LOJAX
First backdoor detected in the wild


HIGH RESEARCH ACTIVITY

Dream Boot
Darth Venamis
Light Eater
Memory Sinkhole
ThinkPwn

1st SecureBoot Bypass
Thunderstrike
SMMbackdoor
PEIbackdoor
SMM->VMM

6 new CVE in BIOS on BlackHat by Alex Matrosov
Intel Boot Guard bypass by Alex Ermolov

APT, ESPIONAGE IS THE MAIN TASK

HOME DEVICES ARE A NEW TARGET

- Undetectable penetration vector
- Even stealthier method of data collection
- Creates more opportunities to attack other devices in a local network
- Good persistence

30% OF APT GROUPS USE LEGAL FRAMEWORKS

METASPLOIT

- Turla
- Lazarus
- OilRig
- Charming Kitten
- Newscaster Team
- APT32
- MuddyWater

COBALT STRIKE

- APT17
- APT10
- TEMP.Periscope
### APT, Espionage is the Main Task

<table>
<thead>
<tr>
<th><strong>AMERICA</strong></th>
<th><strong>EUROPE</strong></th>
<th><strong>APAC</strong></th>
<th><strong>MIDDLE EAST &amp; AFRICA</strong></th>
<th><strong>RUSSIA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>APT28 Russia</td>
<td>Lazarus North Korea</td>
<td>DarkHotel North Korea</td>
<td>OilRig Iran</td>
<td>Equation USA</td>
</tr>
<tr>
<td>Turla Russia</td>
<td>APT28 China</td>
<td>Lazarus North Korea</td>
<td>APT28 Russia</td>
<td>APT10 - China</td>
</tr>
<tr>
<td>Lazarus North Korea</td>
<td>APT15 China</td>
<td>Thrip China</td>
<td>Charming Kitten Iran</td>
<td>APT17 - China</td>
</tr>
<tr>
<td>APT15 China</td>
<td>Tick China</td>
<td>APT32 Vietnam</td>
<td>Orangeworm</td>
<td>PlugX - China</td>
</tr>
<tr>
<td>APT15 China</td>
<td>BlackEnergy Russia</td>
<td>Mustang Panda China</td>
<td>MuddyWater Iran</td>
<td>Prikormka - Ukraine</td>
</tr>
<tr>
<td>APT15 China</td>
<td>BlackEnergy Russia</td>
<td>APT37 North Korea</td>
<td>Slingshot USA</td>
<td>APT28 - Russia</td>
</tr>
<tr>
<td>APT15 China</td>
<td>Dragonfly Russia</td>
<td>Slingshot USA</td>
<td>Newscaster Team Iran</td>
<td>BlackEnergy - Russia</td>
</tr>
<tr>
<td>APT15 China</td>
<td>TEMP.Periscope China</td>
<td>Kimsuky North Korea</td>
<td>APT34 Iran</td>
<td>PowerPool</td>
</tr>
<tr>
<td>APT15 China</td>
<td>Orangeworm</td>
<td>Andriel North Korea</td>
<td>APT33 Iran</td>
<td></td>
</tr>
<tr>
<td>APT15 China</td>
<td>Gorgon Group Pakistan</td>
<td>Tick China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APT15 China</td>
<td>PowerPool</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APT15 China</td>
<td>PowerPool</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Open Sources Only Publish Information on Attacks Originating in Developing Countries**
APT, ESPIONAGE IS THE MAIN TASK

LATE 2017 TO EARLY 2018

FINANCE
- BlackEnergy attacks Japanese banks with ONI ransomware.

COVERT TARGETS
- BadRabbit: mass attacks to conceal real targets under attack.
- VPNFilter: about 500,000 routers in 54 countries were infected. One module was detecting SCADA systems.

POWER ENGINEERING
- BlackEnergy: espionage in SCADA systems without impact
- Triton: framework for manipulating Safety Instrumented System by Schneider Electric with the real accident.

FEBRUARY 2018

OLYMPICS 2018
- APT28: Olympic Destroyer was used to disable the official website of the Olympics and Wi-Fi at the stadium; it also affected live broadcast of the opening ceremony.

FINANCE
- Lazarus puts 9,000 computers and more than 500 servers out of action after Banco de Chile and Bancomext robbery.

JANUARY TO MAY 2018

COVER-UP TRANSACTIONS
- Real sabotaging attacks are covered by smoke walls.
- The infrastructure is prepared in advance to create smoke walls.
PREDICTIONS: HARDWARE VULNERABILITIES AND APT THREATS

FIRMWARE AND SIDE-CHANNEL ATTACKS

- They will become the main research vector of APT attackers.
- Current security solutions are not ready for such challenges.

NEXT TARGET OF FIRMWARE THREATS:

- Motherboard manufacturers
- Vendors that supply hardware to state authorities
- Small/new cloud services

FLATS/HOUSES AND PERSONAL DEVICES

- New priority when protecting secrets and business.
- In the private and public sectors these networks lack due attention.

CRITICAL INFRASTRUCTURE

- Initial penetration through vulnerable network hardware, not phishing.
- Self-replicating ransomware will be used to attack air-gapped networks.
ATTACKS TARGETED AT BANKS

Traditionally, the threat for the financial sector comes from Russian-speaking attackers.
ATTACKS TARGETED AT BANKS: INTERBANK SYSTEMS

JAN 2015
Ecuador, Banco del Austro
$12 million theft

DEC 2016
Turkey, AkBank
Lazarus
$4 million theft

DEC 2017
Russia, bank
Cobalt
$1 million theft
339.5 million RUB attempt

MAY 2018
Chile, Banco de Chile
Presumably Lazarus
$10 million theft

FEB 2016
Bangladesh, Central Bank
Lazarus
$951 million attempt
$81 million theft

APR 2017
Middle East, Latin America
The Shadow Brokers published information about Equation Group’s SWIFT attacks

FEB 2018
Bulgaria, Bulgarian Bank
Cobalt
Unsuccessful attempt

APR 2016
Ukraine, Credit Dnepr bank
Cobalt
$950,830 theft
$10 million attempt
Hong Kong bank (Unknown)
Cobalt

OCT 2017
Taiwan, Far Eastern International Bank
Lazarus
$60 million attempt, most were recovered
Nepal, NIC Asia Bank
Presumably Lazarus
$4.4 million attempt
$580,000 theft

FEB 2018
India, Punjab National Bank
Lazarus
$1.7 million theft
India, City Union Bank
$1.87 million theft

OCT 2015
Vietnam, Tien Phong Bank (TPBank)
$1.36 million attempt

FEB 2017
Poland, Banks
Lazarus

JAN 2018
Mexico, Bancomext
Presumably Lazarus
$110 million theft

APR 2018
Mexican banks
Mexican central bank informed about $18 million SWIFT thefts

SWIFT
2 groups are the threat to SWIFT: Lazarus and Cobalt
3 times more incidents
$26 mln is the average volume of a theft attempt

LOCAL INTERBANK SYSTEMS
They are also targets, but there is no data on the attacks
ARM CBR was attacked only once by MoneyTaker
ATTACKS TARGETED AT BANKS: INTERBANK SYSTEMS

ATTACKS ON ATMS

They draw attackers’ attention again. Two groups: MoneyTaker and Silence have created new Trojans for this purpose.

CARD PROCESSING

This is still the main way to monetize access to the banking network in all groups.

Lazarus started using this theft method.

PAYMENT GATEWAYS

This theft method is only used by the Cobalt group.

There were no new attempts after the 2017 attacks.

RUSSIA IS NOT A PRIORITY ANYMORE

All Russian-speaking groups started with attacks in Russia.

Attacks in Russia are not the priority anymore, and all groups attack foreign banks.
PREDICTIONS: ATTACKS TARGETED AT BANKS

**ATTACKS OUTSIDE RUSSIA**

- First and foremost, we should expect a lot of attacks from Silence.
- Local cybercrime groups will start conducting similar attacks. Above all, we expect growth in the APAC Region.

**COMBINED THEFT METHODS**

- Lazarus should be expected to steal via SWIFT and card processing at the same time.
- Cybercrime groups will steal via ATMs and card processing.
- Using ransomware after attack completion can become a trend.

**INITIAL PENETRATION VECTOR IS CHANGING**

- Phishing is still the main vector.
- Some groups will start trying to penetrate banks through web vulnerabilities and vulnerable network hardware.

**NEW GROUPS**

- After the arrests of Cobalt and Fin7 participants, we can expect new criminal groups to appear.
- Topplel and RTM are the most likely ones to form new groups.
PC TROJANS

STAGNANT DEVELOPMENT WORLDWIDE

- Activity and efficiency of banking Trojans fall all over the world.
- Arrest of Neverquest, GozNym, and Andromeda loader authors hit hard.
- Owners of large botnets use them to install ransomware.

LOCAL NATURE

- Each threat became local and affects 3 to 5 countries on average.

AUTOMATIC TRANSFER SYSTEMS (ATS)

- New: BackSwap is the only Trojan with new techniques: a developer’s console and a bookmarklet.
ANDROID TROJANS

SECURITY BY GOOGLE

• The main reason for restraining Android threats.
• Old Trojan versions do not work on new Android versions.

SLOWDOWN ABROAD

• 5 Trojans—Xbot, Abrvall, Vasya, UfoBot, Reich—are no longer used due to poor support.
• The most active developer, GanjaMan, who created the most popular versions of Trojans, was blocked, and his developments are no longer used.

STAGNANT DEVELOPMENT IN RUSSIA

• The owners of the two largest botnets, Cron and Tiny.z, were arrested
• Honli botnet was disabled.
• Number of thefts became three times smaller, and damage decreased by 77%.
• Average amount of damage was reduced from 11 to 7 thousand.

TROJANS WITH WEB FAKE GLOBALY

Easy | Exobot 2.0 | CryEye | Cannabis
Fmif | AndyBot | Loki v2 | Nero Banker
Sagawa | Agent.cj | Maza-in | Loki v2
Alien bot | Rello | Red Alert v2
ATM THREATS

ATM JACKPOTTING

- “New” ATM threat.
- Attackers get physical access to an ATM.
- They plug a microcomputer of a smartphone into the USB/COM port of a dispenser.

CUTLET MAKER

- The main reason for the increase in theft using this method.
- The software is provided in one package with the detailed instruction and an Android app.
- Hacker versions surfaced and led to wider distribution.

MR. MARKAS

- The main software developer for ATM Jackpotting.
### CARDING

<table>
<thead>
<tr>
<th></th>
<th>Text data</th>
<th>Dumps</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number</td>
<td>10 218 489</td>
<td>16 927 777</td>
<td>27 146 266</td>
</tr>
<tr>
<td>Market volume</td>
<td>$95 590 424</td>
<td>$567 791 443</td>
<td>$663 381 867</td>
</tr>
<tr>
<td>Lowest price</td>
<td>$0.75</td>
<td>$0.5</td>
<td></td>
</tr>
<tr>
<td>Highest price</td>
<td>$99.99</td>
<td>$295</td>
<td></td>
</tr>
<tr>
<td>Average price</td>
<td>$9.35</td>
<td>$33.54</td>
<td></td>
</tr>
<tr>
<td>Median</td>
<td>$8</td>
<td>$25</td>
<td></td>
</tr>
</tbody>
</table>

1.8 MLN CARDS WERE UPLOADED TO CARDSHOPS

- 62% of data sold is connected to card data dumps
- POS Trojans are the main method of getting the dumps
- Text data accounts for just 17% of all card-related market.
POS THREAT

2017

01.06.2017
Detecting of new POS malware LockPos

10.09.2017
Sale of Sisyphus POS
Threat actor - Refreshers
Forum - exploit.in

15.11.2017
Attacks on pubs and restaurant using Alina POS

01.10.2017
Lazarus cybercrime group attacks on South Korea with using of RatankbaPOS

01.12.2017
Sale of source codes of NCR Radiant (RPOS) software
Threat actor - discorb
Forum - exploit.in

08.05.2018
Leak of POS malware source code
Threat actor - Unsigned
Forum - exploit.in

04.07.2018
Searching for RDP with access to POS
Threat actor - beau
Forum - exploit.in

2018

01.12.2017
Detecting of new malware "UDPos"

15.02.2018
Detecting of new malware "UDPos"

10.11.2017
Detection of new POS-malware "GratefulPOS"

08.02.2018
Sale of POS sniffer source code
Threat actor - ftp_admin
Forum - exploit.in

13.04.2018
PoS Malware "Treasure Hunted" Source Code Leaked
Threat actor - crossair
Forum - exploit.in

08.06.2018
Sale of source code for malware for MagicPos
Threat actor - cocofresh
Forum - exploit.in
PREDICTIONS

**ROUTERS ARE A POINT OF GROWTH**

- Wi-Fi in restaurants will become the main method of POS terminal penetration and infection.
- Forwarding to phishing by manipulating traffic at the router level.

**ATM JACKPOTTING**

- In various countries Cutlet is the main tool to attack ATMs with physical access.
- We should expect growth in the number of logical attacks following banks hacking. All groups have relevant Trojans in their armory now.

**BANKING TROJANS**

- Android Trojans will start to attack organizations through contextual advertising.
- Android will continue to replace PC Trojans.
- PC Trojan BackSwap and IcedID can become a significant threat for banks in the USA and Europe.

**DAMAGE FOR BANK CUSTOMERS**

- There will be a reduction in all areas except for targeted attacks.
- Phishing will be the main source of damage.
THREATS FOR THE CRYPTOCURRENCY MARKET: MANIPULATION WITH THE CRYPTOCURRENCY EXCHANGE RATE

ATTACKERS’ TACTICS

- Phishing website disguised as the Chinese exchange Binance
- Collection of logins and passwords of traders
- Generation of API keys to automate operations on the exchange

- In 2 minutes, generation of trader applications for the little-known cryptocurrency Viacoin
- In 30 minutes, Viacoin rate jumped by 143%
- Selling Viacoin via Bitcoin with the inflated rate
THREATS FOR THE CRYPTOocurrency MARKET: 51% ATTACK

Double-spending is considered to be the biggest threat to the system.

Having 51% of computing power, the attacker can create a stealthy alternative blockchain and use it to confirm an attacker’s own transactions.

<table>
<thead>
<tr>
<th>APRIL 4</th>
<th>MAY 18</th>
<th>MAY 22</th>
<th>JUNE 3</th>
<th>JUNE 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERGE</td>
<td>BITCOIN GOLD</td>
<td>VERGE</td>
<td>ZENCASH</td>
<td>LITECOIN CASH</td>
</tr>
<tr>
<td>An attacker could mine $1 million worth of cryptocurrency.</td>
<td>An attacker could mine $18 million worth of cryptocurrency.</td>
<td>SuperNova reported that Verge was under 51% attack and all correct blocks are rejected.</td>
<td>An attacker could mine $550,000 worth of cryptocurrency.</td>
<td>Litcoin (LTC) fork also faced 51% attack.</td>
</tr>
</tbody>
</table>
THREATS FOR THE CRYPTOocurrency MARKET:
TARGETED HACKING OF CRYPTO EXCHANGES

NUMBER OF THEFTS BECAME 5 TIMES LARGER
COMPARSED TO THE PREVIOUS YEAR

2016
$168 MLN

2017
$877 MLN
61% of the total is stolen from Coincheck

NORTH KOREA IS THE MAIN THREAT

• 5 out of 10 thefts are believed to be connected to Lazarus
• Most exchanges which have become victims are from South Korea
• YouBit/Yapizon went bankrupt.

THIRD PARTY ATTRIBUTION FROM OPEN SOURCE

<table>
<thead>
<tr>
<th>Date</th>
<th>Name of Project</th>
<th>Country</th>
<th>Criminal group</th>
<th>Stolen in cryptocurrencies</th>
<th>Stolen in USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 2017</td>
<td>Bithumb</td>
<td>South Korea</td>
<td>Unknown</td>
<td>-</td>
<td>$7 mln</td>
</tr>
<tr>
<td>Apr 2017</td>
<td>YouBit</td>
<td>South Korea</td>
<td>Unknown</td>
<td>-</td>
<td>$5.6 mln</td>
</tr>
<tr>
<td>Apr 2017</td>
<td>Yapizon</td>
<td>South Korea</td>
<td>Lazarus</td>
<td>3,816 BTC</td>
<td>$5.3 mln</td>
</tr>
<tr>
<td>Aug 2017</td>
<td>Ether Delta</td>
<td>-</td>
<td>Unknown</td>
<td>-</td>
<td>$277 k</td>
</tr>
<tr>
<td>Aug 2017</td>
<td>OKEx</td>
<td>Hong Kong</td>
<td>Unknown</td>
<td>-</td>
<td>$3 mln</td>
</tr>
<tr>
<td>Sep 2017</td>
<td>Coinis</td>
<td>South Korea</td>
<td>Lazarus</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Dec 2017</td>
<td>YouBit</td>
<td>South Korea</td>
<td>Lazarus</td>
<td>17% of assets</td>
<td>-</td>
</tr>
<tr>
<td>Jan 2018</td>
<td>Coincheck</td>
<td>Japan</td>
<td>Lazarus</td>
<td>523 mln NEM</td>
<td>$534 mln</td>
</tr>
<tr>
<td>Feb 2018</td>
<td>Bitgrail</td>
<td>Italy</td>
<td>Unknown</td>
<td>17 mln NANO</td>
<td>$170 mln</td>
</tr>
<tr>
<td>Jun 2018</td>
<td>Bithumb</td>
<td>South Korea</td>
<td>Lazarus</td>
<td>-</td>
<td>$32 mln</td>
</tr>
<tr>
<td>Jun 2018</td>
<td>Coinrail</td>
<td>South Korea</td>
<td>Unknown</td>
<td>11 types of cryptocurrency</td>
<td>$37 mln</td>
</tr>
<tr>
<td>Jun 2018</td>
<td>Bancor</td>
<td>-</td>
<td>Unknown</td>
<td>-</td>
<td>$23 mln</td>
</tr>
<tr>
<td>Sept 2018</td>
<td>Zaif</td>
<td>Japan</td>
<td>Unknown</td>
<td>-</td>
<td>$60 mln</td>
</tr>
</tbody>
</table>

TOTAL $877 MLN
**PREDICTIONS**

**REDUCTION OF MINING**

- Cryptojacking boom is over.
- Trojans are no longer efficient for mining.

**NEW ATTACKERS**

- Silence, MoneyTaker, and Cobalt may conduct several successful targeted attacks on exchanges and the largest miners.

**THE LARGEST MINERS**

- They will become the main target of the pro-government attackers to control 51% of power and take over the cryptocurrency control.

**ICO**

- It is still the target for hackers.
- However, the number of attacks will decline.