Booby Trapping Boxes

Running Private Services as a High Value Target

Version 2.0.1
August 11th 2016

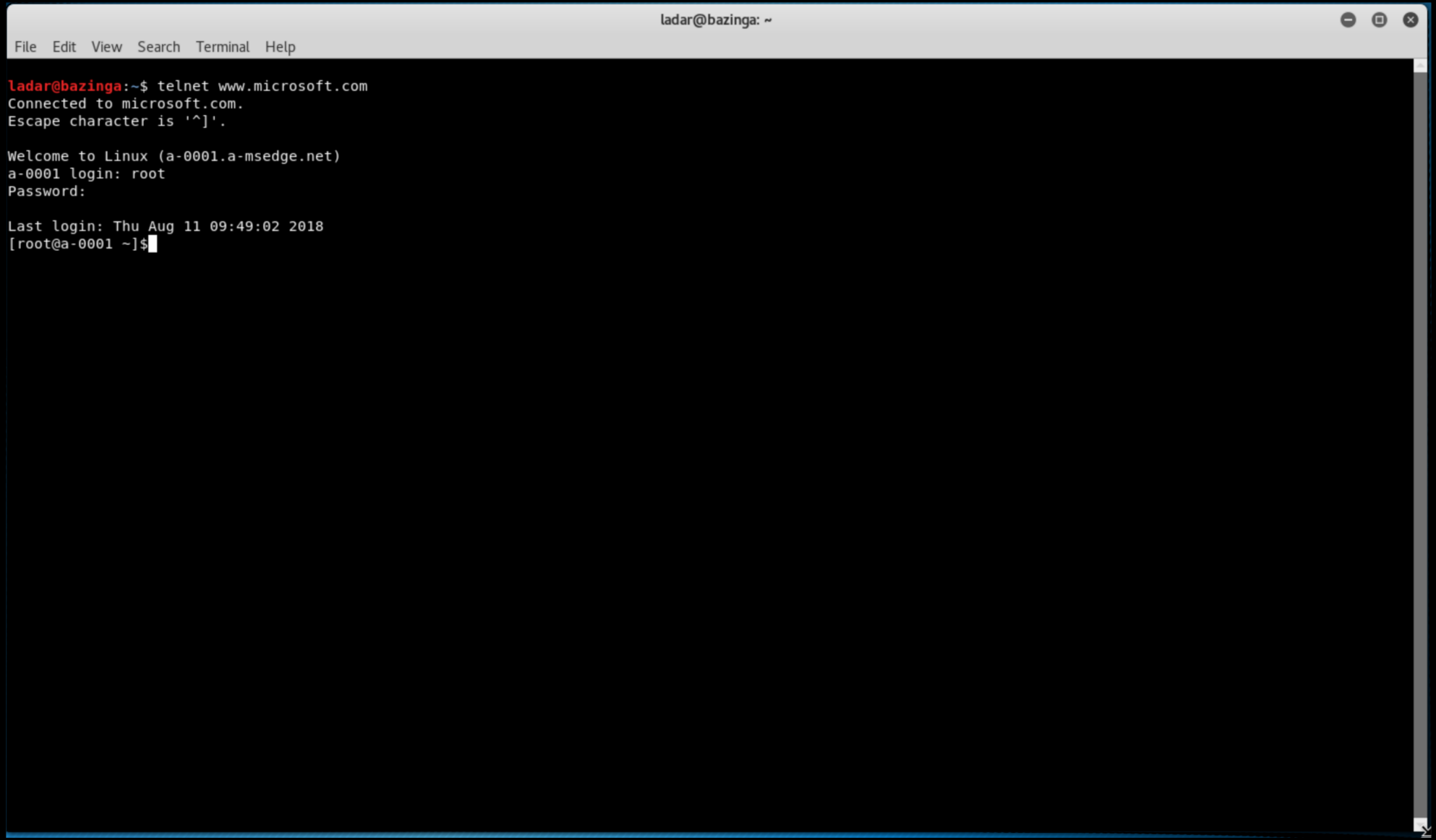


Ladar Levison

Owner and Operator, Lavabit LLC

Hon1bo Tails

Proprietor, Hacking and Coffee

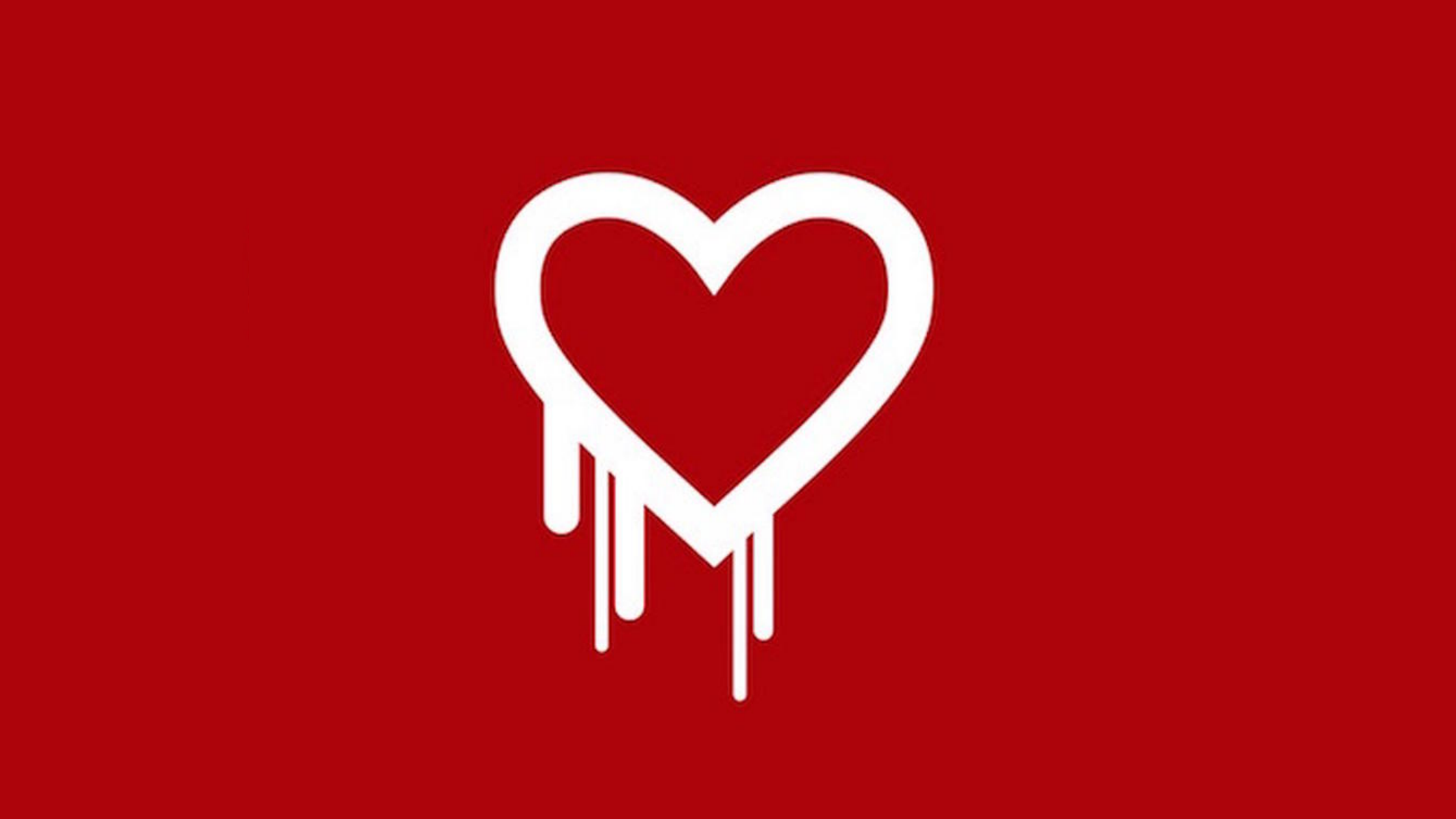

ladar@bazinga: ~
File Edit View Search Terminal Help
ladar@bazinga:~$ telnet www.microsoft.com
Connected to microsoft.com.
Escape character is '^]'.
Welcome to Linux (a-0001.a-msedge.net)
a-0001 login: root
Password:
Last login: Thu Aug 11 09:49:02 2018
[root@a-0001 ~]$

APPLIED CRYPTOGRAPHY



Protocols, Algorithms, and Source Code in C

BRUCE SCHNEIER




ALTAIR 8800 COMPUTER
ALTAIR DIS



tom's HARDWARE

Hacker Finds Hidden 'God Mode' on Old x86 CPUs

by Paul Wagenseil August 9, 2018 at 5:06 PM

LAS VEGAS — Some x86 CPUs have hidden backdoors that let you seize root by sending a command to an undocumented RISC core that manages the main CPU, security researcher Christopher Domas told the Black Hat conference here Thursday (Aug. 9).

The command — ".byte 0x0f, 0x3f" in Linux — "isn't supposed to exist, doesn't have a name, and gives you root right away," Domas said, adding that he calls it "God Mode."

The backdoor completely breaks the protection-ring model of operating-system security, in which the OS kernel runs in ring 0, device drivers run in rings 1 and 2, and user applications and interfaces ("userland") run in ring 3, furthest from the kernel and with the least privileges. To put it simply, Domas' God Mode takes you from the outermost to the innermost ring in four bytes.

"We have direct ring 3 to ring 0 hardware privilege escalation," Domas said. "This has never been done."

That's because of the hidden RISC chip, which lives so far down on the bare metal that Domas half-joked that it ought to be thought of as a new, deeper ring of privilege, following the theory that hypervisors and chip-management systems can be considered ring -1 or ring -2.

"This is really ring -4," he said. "It's a secret, co-located core buried alongside the x86 chip. It has unrestricted access to the x86."

The good news is that, as far as Domas knows, this backdoor exists only on VIA C3 Nehemiah chips made in 2003 and used in embedded systems and thin clients. The bad news is that it's entirely possible that such hidden backdoors exist on many other chipsets.

"These black boxes that we're trusting are things that we have no way to look into," he said. "These backdoors probably exist elsewhere."

Domas discovered the backdoor, which exists on VIA C3 Nehemiah chips made in 2003, by combing through filed patents. He found one — US8341419 — that mentioned jumping from ring 3 to ring 0 and protecting the machine from exploits of model-specific registers (MSRs),

Positive Technologies - learn and secure

August 28, 2017

Disabling Intel ME 11 via undocumented mode



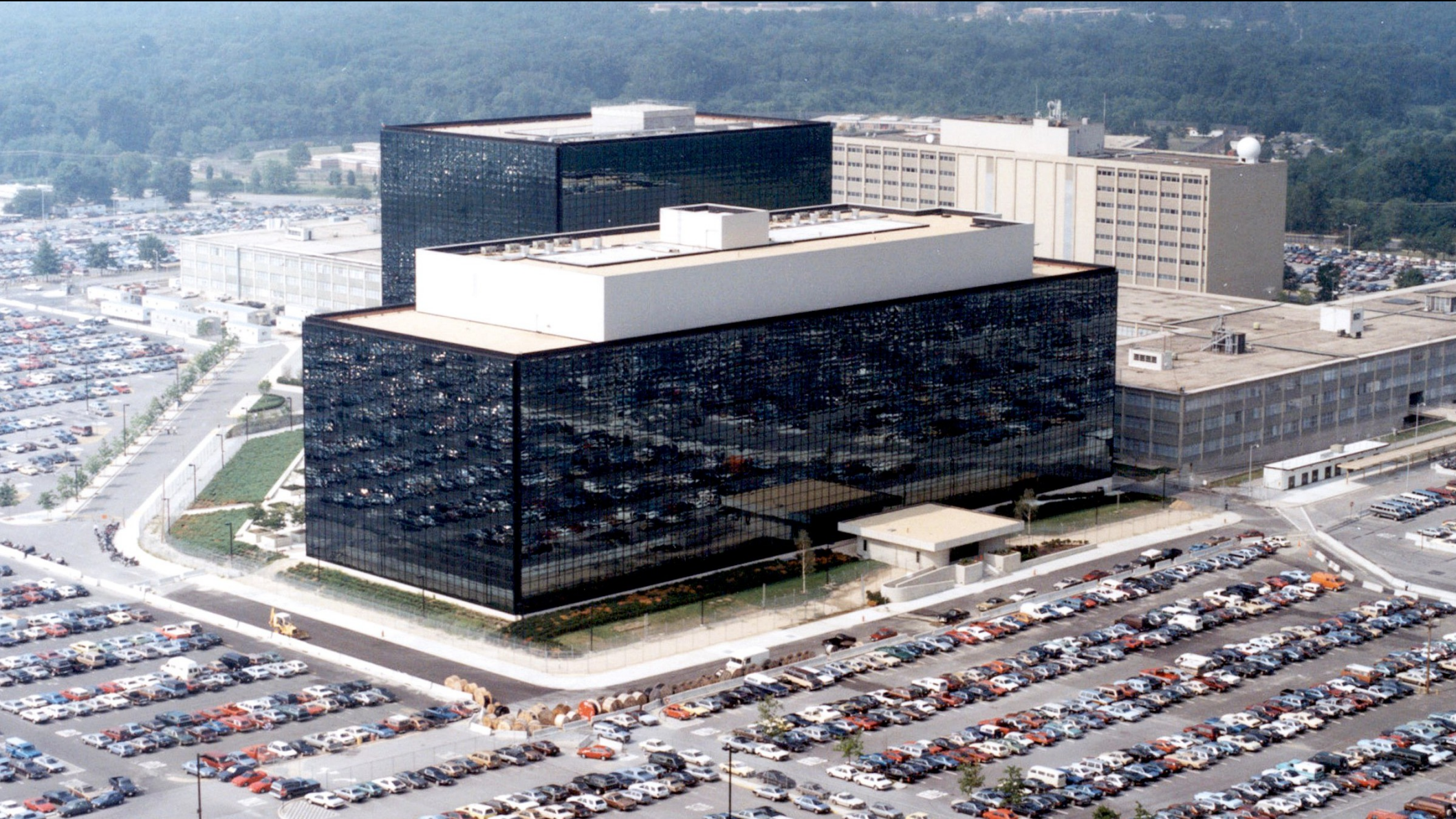
Our team of Positive Technologies researchers has delved deep into the internal architecture of Intel Management Engine (ME) 11, revealing a mechanism that can disable Intel ME after hardware is initialized and the main processor starts. In this article, we describe how we discovered this undocumented mode and how it is connected with the U.S. government's High Assurance Platform (HAP) program.

Disclaimer: The methods described here are risky and may damage or destroy your computer. We take no responsibility for any attempts inspired by our work and do not guarantee the operability of anything. For those who are aware of the risks and decide to experiment anyway, we recommend using an SPI programmer.

Introduction

Intel Management Engine is a proprietary technology that consists of a microcontroller integrated into the Platform Controller Hub (PCH) chip and a set of built-in peripherals. The PCH carries almost all communication between the processor and external devices; therefore Intel ME has access to almost all data on the computer. The ability to execute third-party code on Intel ME would allow for a complete compromise of the platform. We see increasing interest in Intel ME internals from researchers all over the world. One of the reasons is the transition of this subsystem to new hardware (x86) and software (modified MINIX as an operating system). The x86 platform allows researchers to make use of the full power of binary code analysis tools. Previously, firmware analysis was difficult because earlier versions of ME were based on an ARCompact microcontroller with an unfamiliar set of instructions.

Unfortunately, analysis of Intel ME 11 was previously impossible because the executable modules are compressed by Huffman codes with unknown tables. Nonetheless, our research team (Dmitry Sklyarov, Mark Ermolov, and Maxim Goryachy) managed to recover these tables and created a utility for unpacking images. The utility is available on our GitHub page.



FIPS PUB 140-2

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supercedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**



Common Criteria for Information Technology Security Evaluation

1.4 Security Level 4

Security Level 4 provides the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and zeroize CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

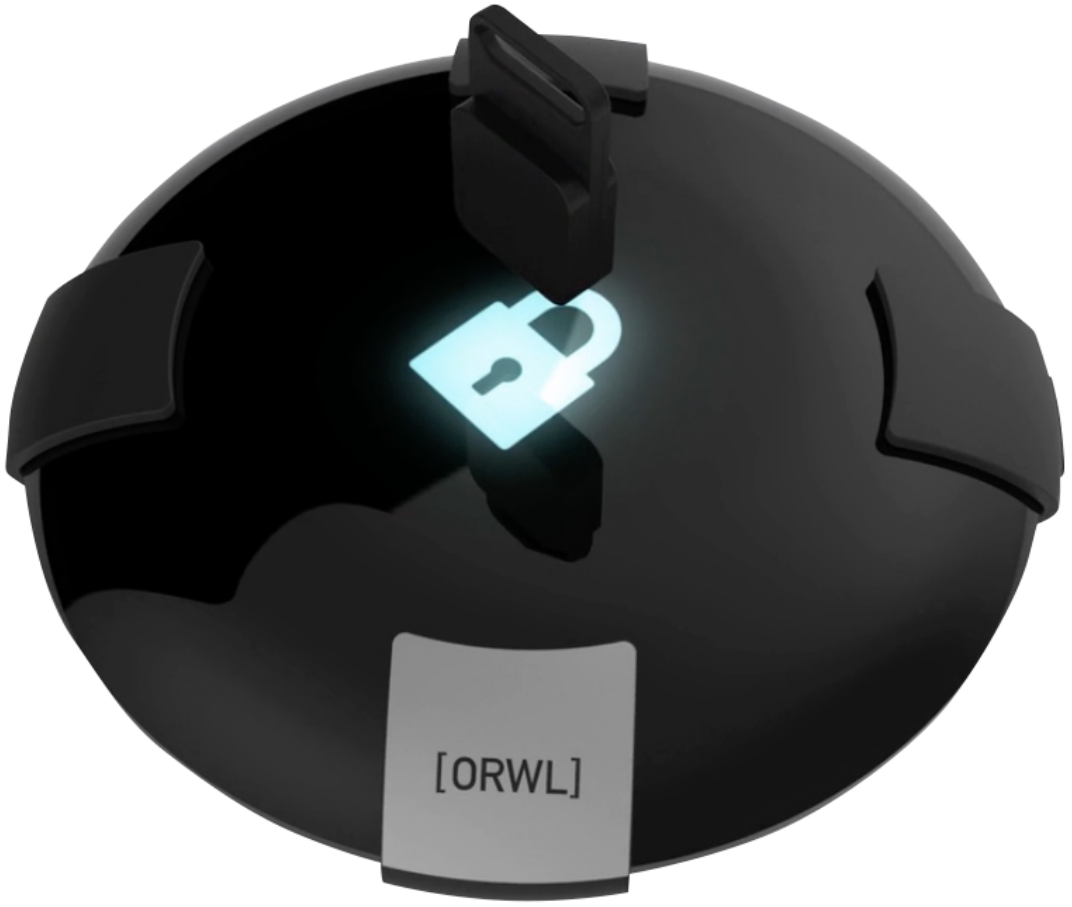
Security Level 4 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that

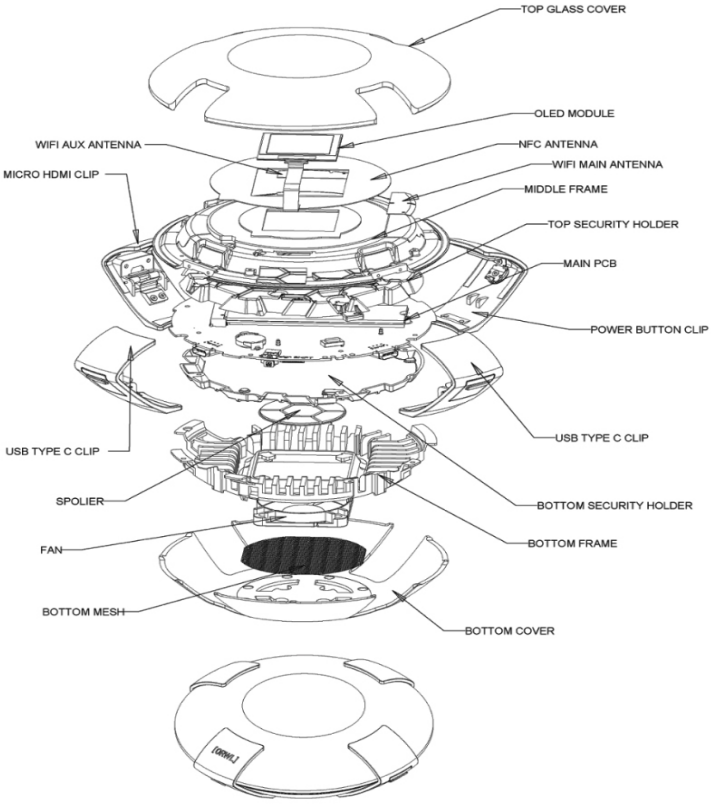
- meets the functional requirements specified for Security Level 3 and
- is evaluated at the CC evaluation assurance level EAL4 (or higher).

An equivalent evaluated trusted operating system may be used.

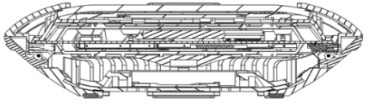



Luna SA
SafeNet





SYSTEM UNIT



SECTION DIAGRAM




DELL

ars TECHNICA

AT LEAST THEY PICK UP THE EXTRA SHIPPING —

Photos of an NSA "upgrade" factory show Cisco router getting implant

Servers, routers get "beacons" implanted at secret locations by NSA's TAO team.

SEAN GALLAGHER - 5/14/2014, 2:30 PM



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

NSA techs perform an unauthorized field upgrade to Cisco hardware in these 2010 photos from an NSA document.

258

A document included in the trove of National Security Agency files released with Glenn Greenwald's book *No Place to Hide* details how the agency's Tailored Access Operations (TAO) unit and other NSA employees intercept servers, routers, and other network gear being shipped to organizations targeted for surveillance and install covert implant firmware onto them before they're delivered.



FURTHER READING
NSA hacker in residence dishes on how to "hunt" system admins

These Trojan horse systems were described by an NSA manager as being "some of the most

ars TECHNICA

Report: Apple designing its own servers to avoid snooping

Apple suspects that servers are intercepted and modified during shipping.

JON BRODKIN - 3/24/2016, 9:09 AM

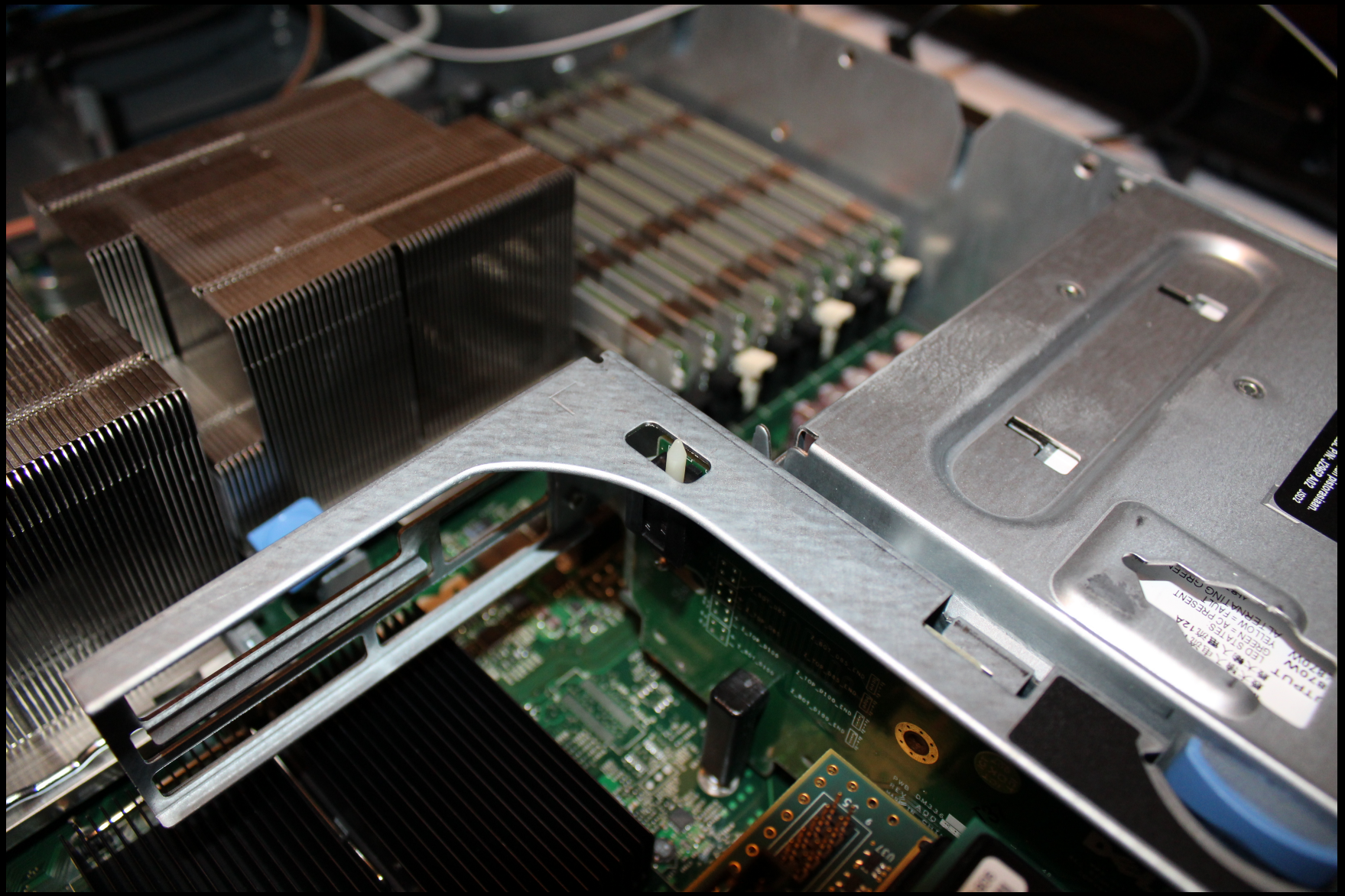
One of Facebook's data centers filled with custom-designed servers.

Apple has begun designing its own servers partly because of suspicions that hardware is being intercepted before it gets delivered to Apple, according to a report yesterday from The Information.

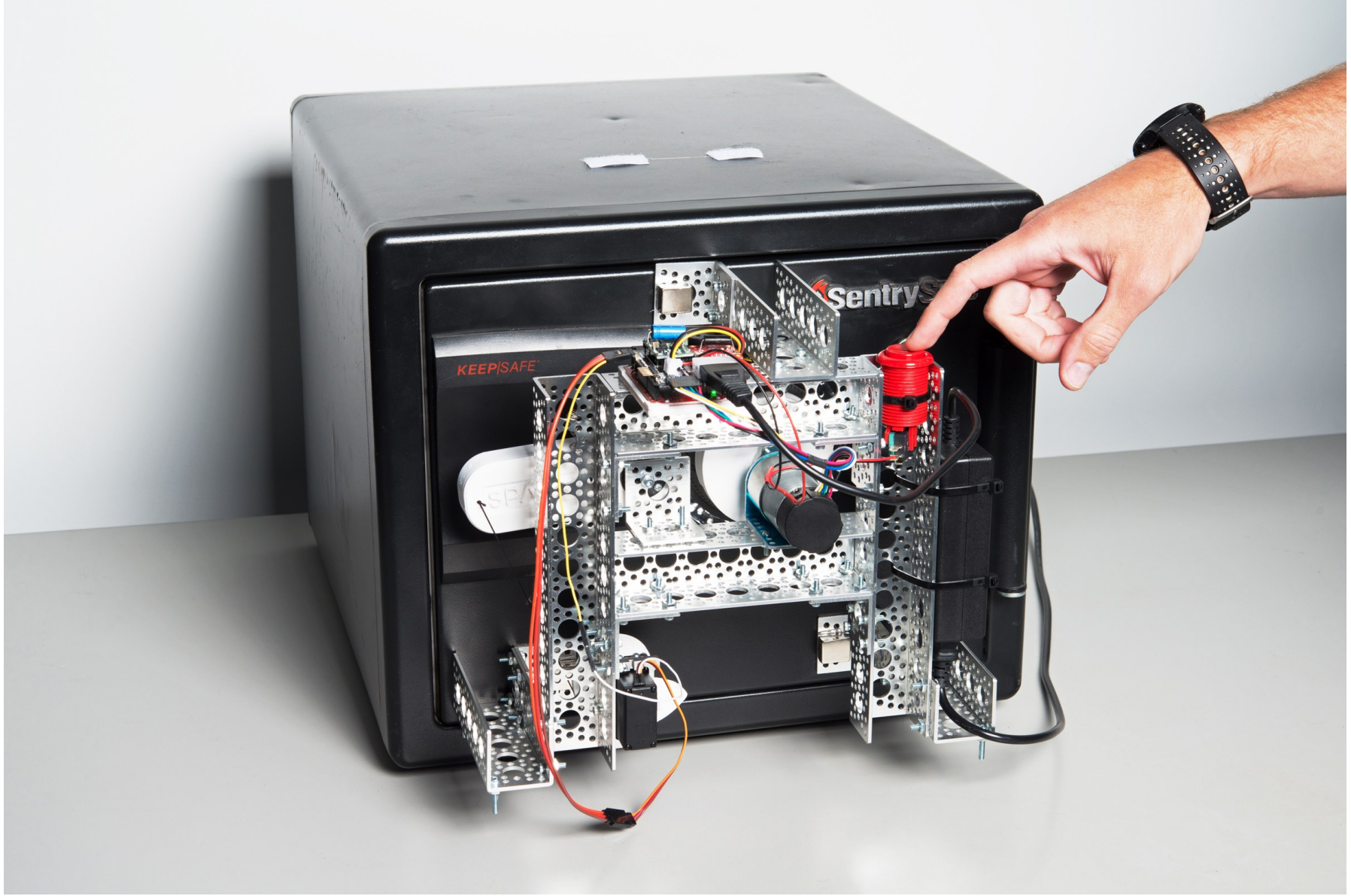
"Apple has long suspected that servers it ordered from the traditional supply chain were intercepted during shipping, with additional chips and firmware added to them by unknown third parties in order to make them vulnerable to infiltration, according to a person familiar with the matter," the report said. "At one point, Apple even assigned people to take photographs of motherboards and annotate the function of each chip, explaining why it was supposed to be there. Building its own servers with motherboards it designed would be the most surefire way for Apple to prevent unauthorized snooping via extra chips."

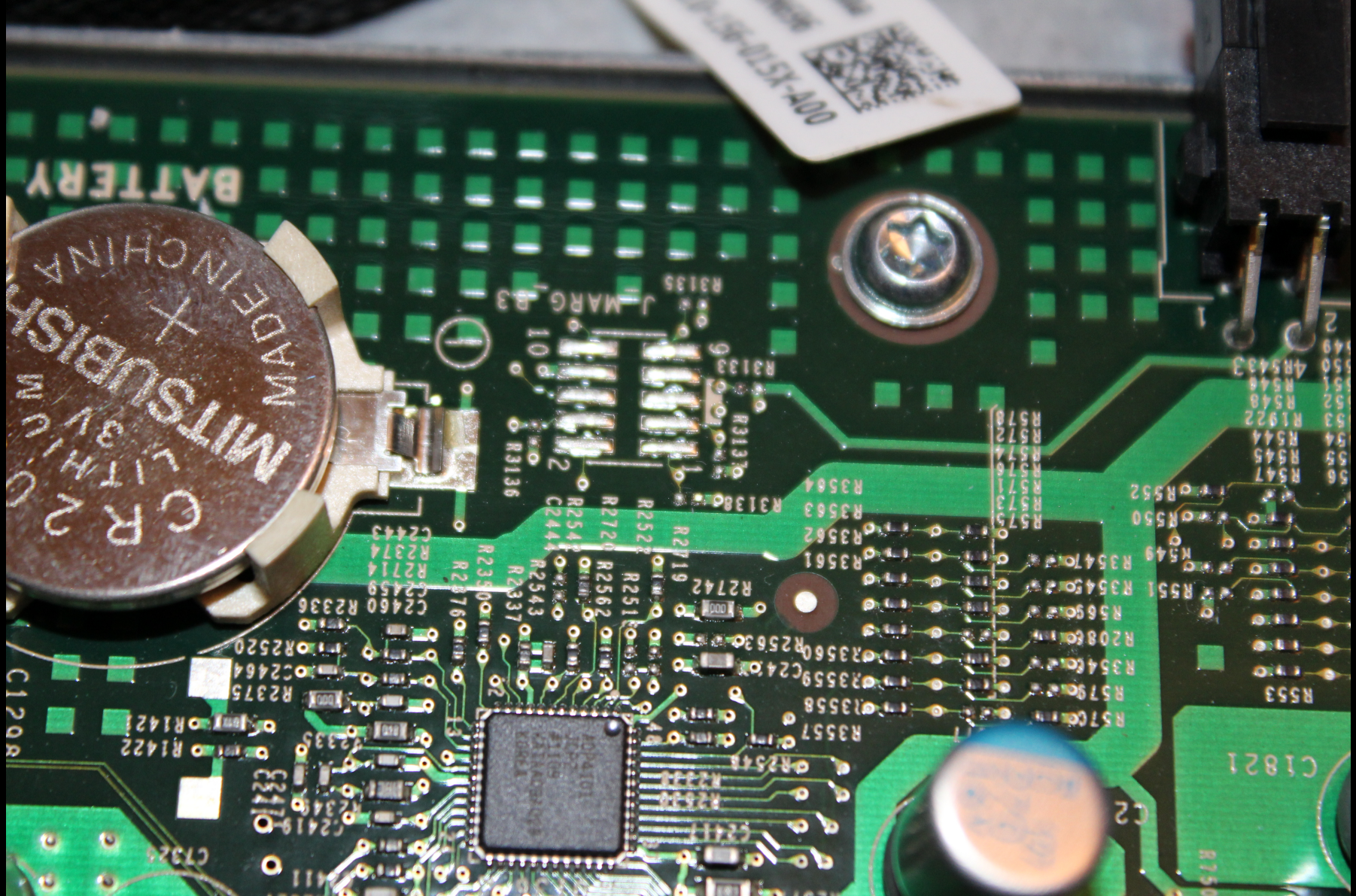
Servers:

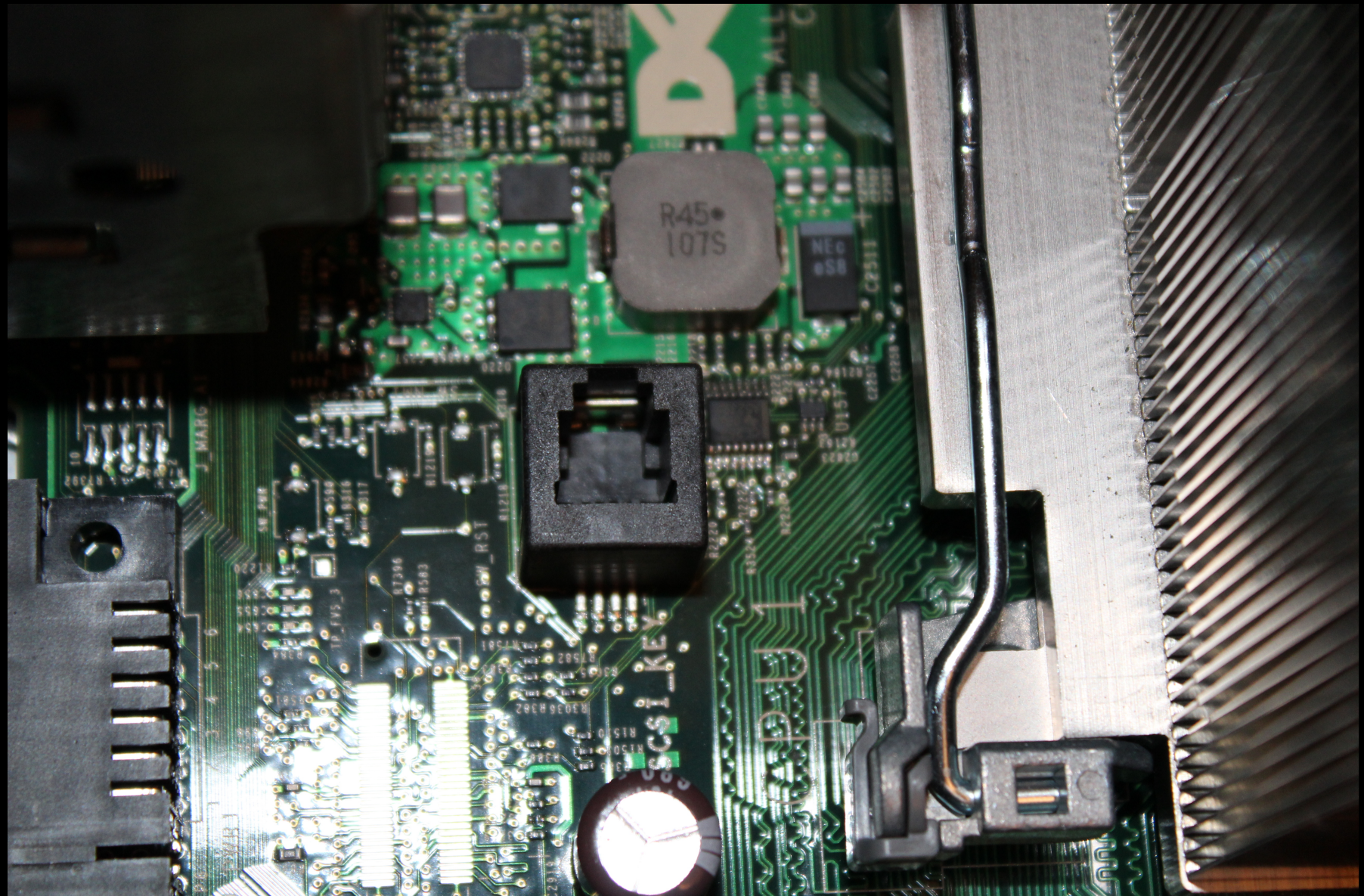
Some of the servers listed in the exploit catalog included HP's Proliant 380DL G5 server, which is targeted by an IRONCHEF tool to extract data using two-way RF communication. With DIETYBOUNCE, the NSA exploits a BIOS vulnerability in Dell's PowerEdge servers 1850, 2850, 1950, 2950 by using remote access or inserting an USB stick. Dell PowerEdge 1950 and 2950 have a JTAG debugging interface that the NSA exploits via GODSURGE. All of the server exploits are listed at a cost of $0 per unit except for GODSURGE, which costs $500 for hardware and installation.



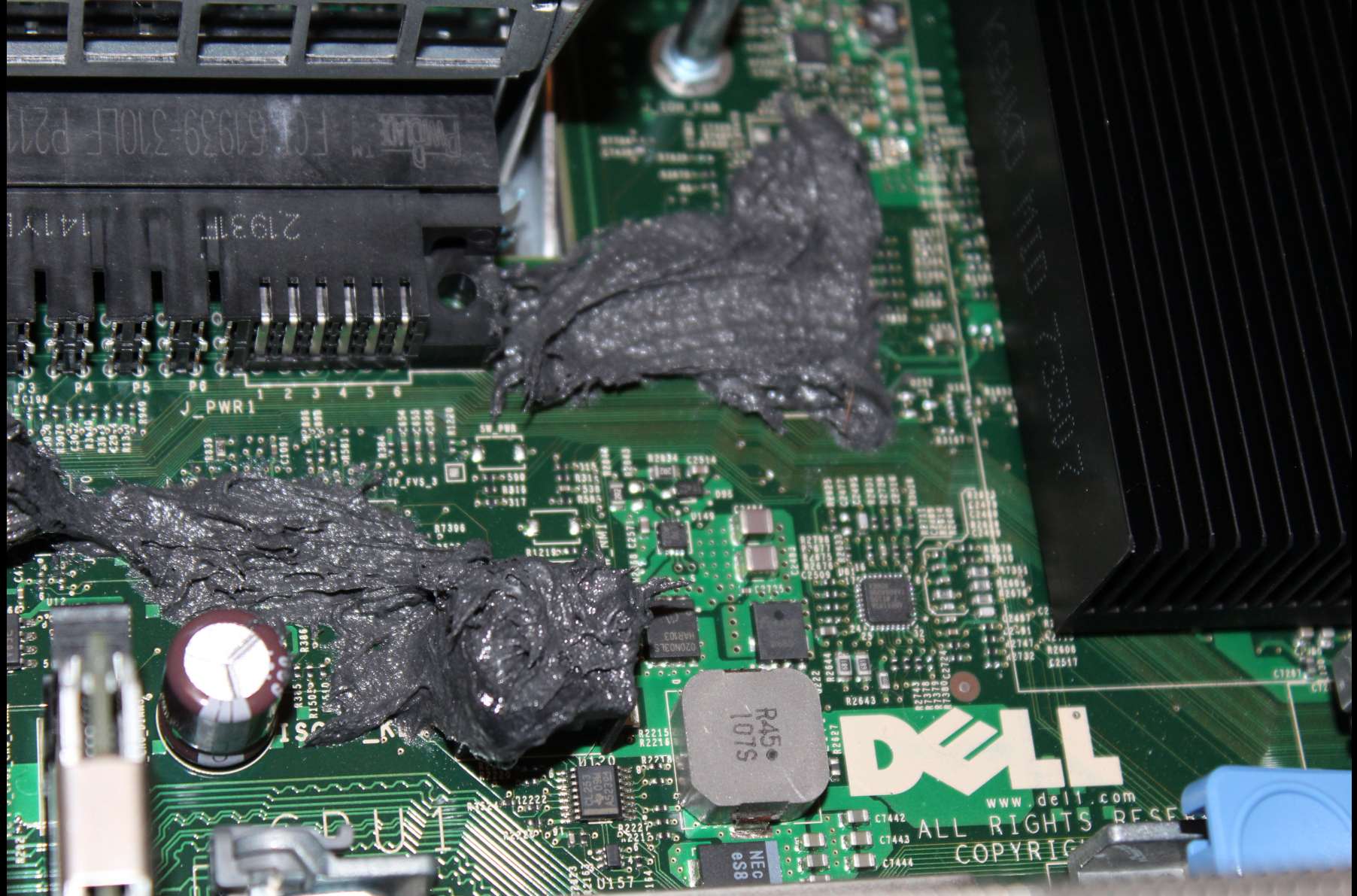



KEEP|SAFE


BATTERY
MADE IN CHINA
MITSUBISHI
CR2
LITHIUM
3V
J MARG B3
C1821


R45
107S
NEC
eSB
J_MARG
CS_KEY


52R3
52R3
J_COM1
SAS
IBM


J_PWR1
DELL
www.dell.com
ALL RIGHTS RESE
COPYRIG


FAN4
FAN5
C 127
270
16V
1R5
102S
NEc
eS8
R45
C14X

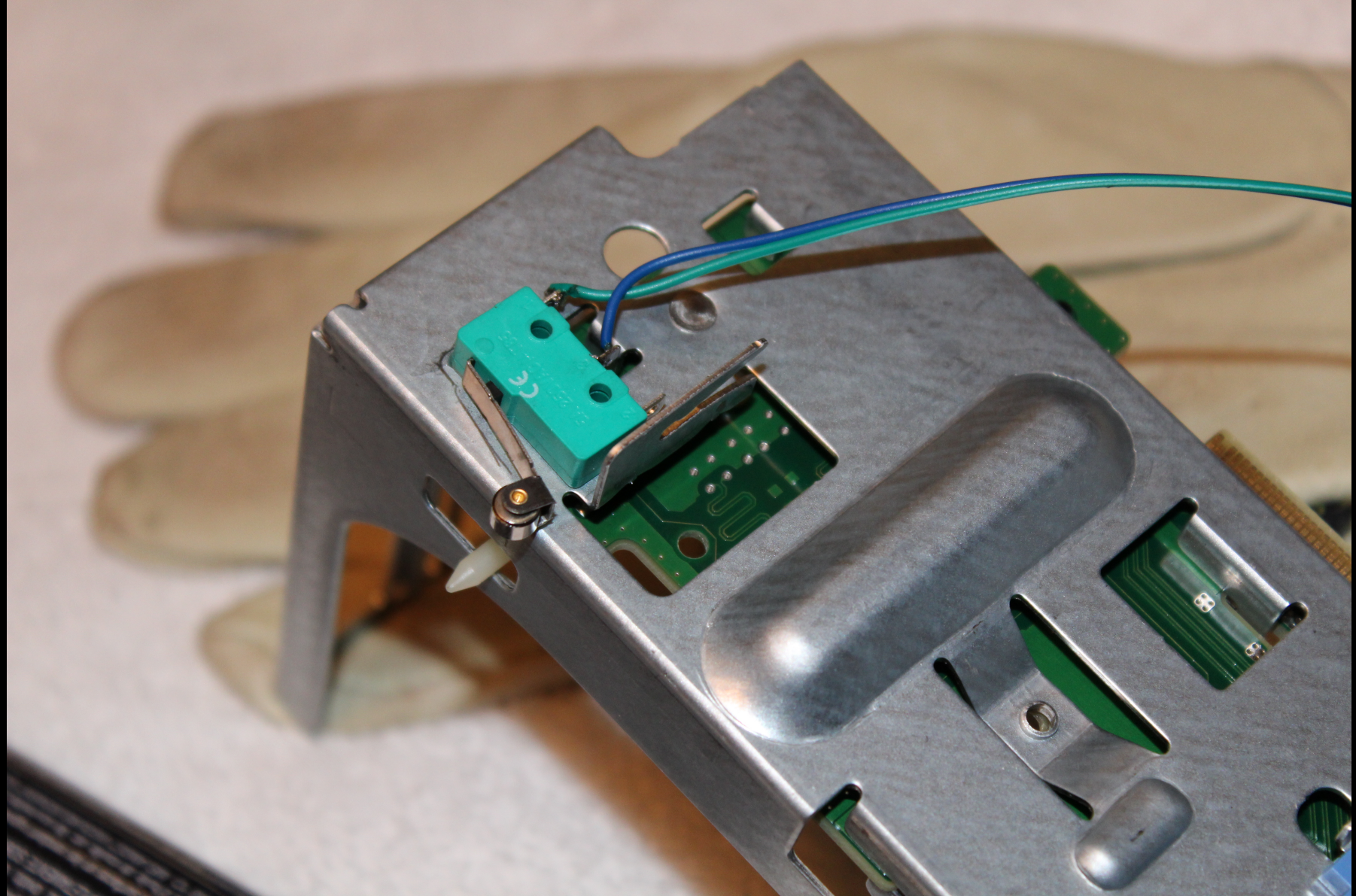

RISER 1
DELL
www.dell.com
COPYRIGHT 2007
ALL RIGHTS RESERVED
PWB R559C REVA00
UL94V-0
MADE IN CHINA
CHINA
DP/N
0R557C
CN-0R557C-13740-
157-02VU-A00
NYKS NM14
1114-08
02B
52R3
52R
52R3
52R3
52R3
R100

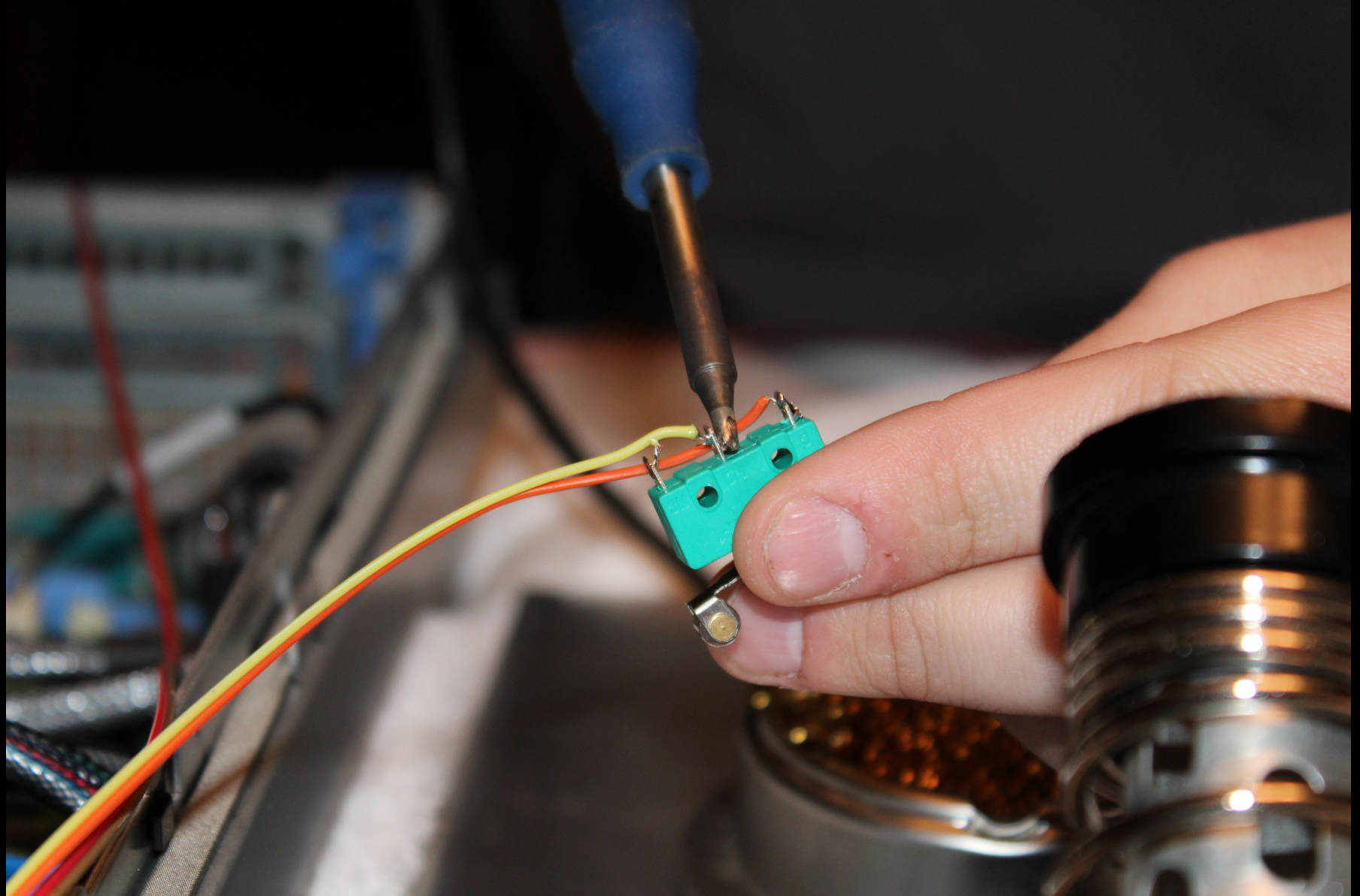

Internal SD Module
SD
USB

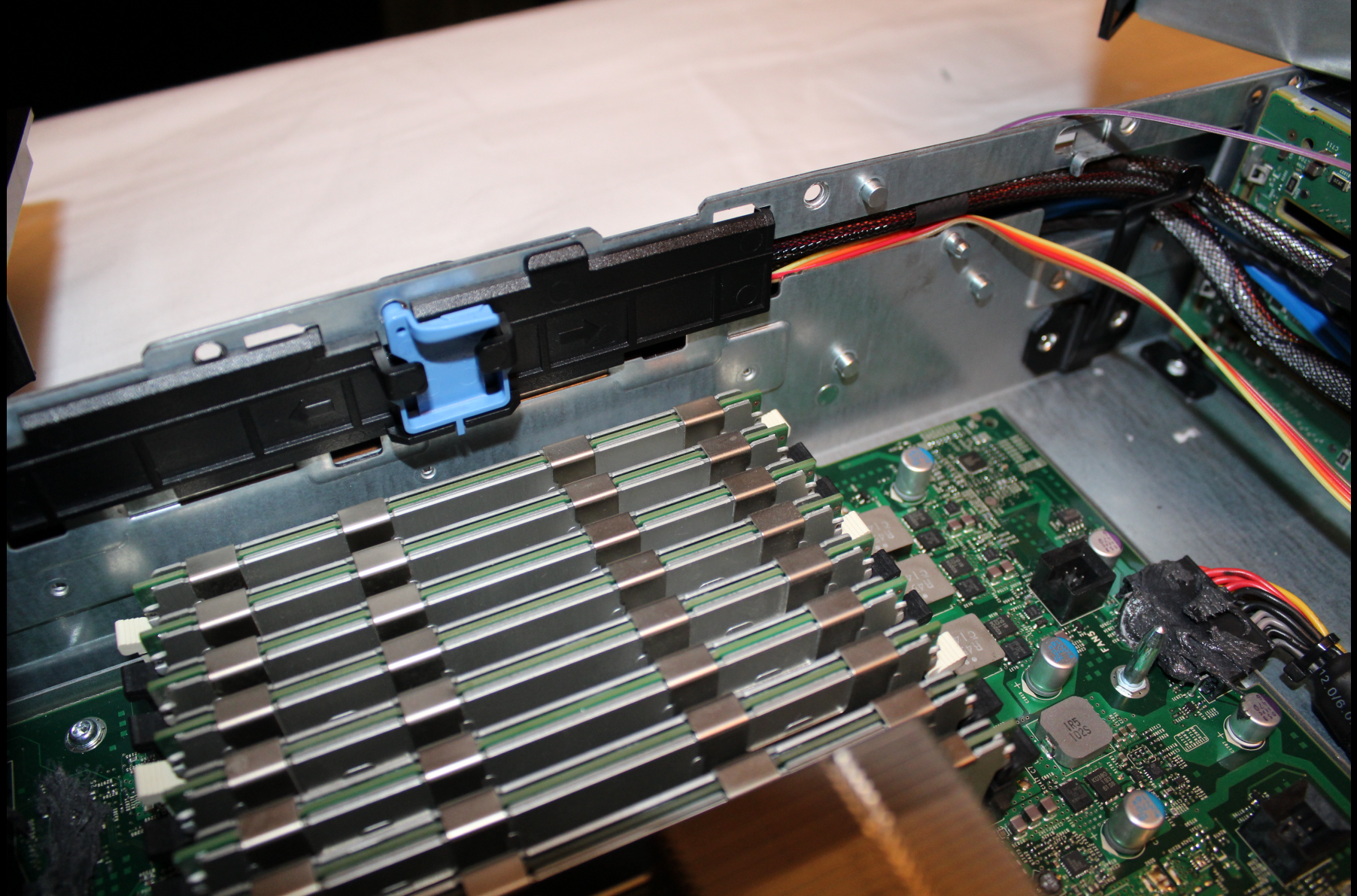

PC·7®
HEAVY DUTY
SERVICIO PESADO
TRÈS ROBUSTE
EPOXY
EPÓXICA
ÉPOXYDE
PC·7®
B
NO SAG, NO DRIP
NO HUNDE, NO GOTEA
PAS D'AFFAISSEMENT,
PAS DE COULURE
WATERPROOF / IMPERMÉABLE / ÉTANCHE
Multipurpose / Multiusos / Universelle
1:1 MIX / MEZCLE / MÉLANGEZ
A+B= 2 oz. (56 g.) UNIT NET WT.
PC-Products® — Protective Coating Co. (Since 1954) Allentown, PA USA 18102
"The Impossible Made Easy®" www.pcepoxy.com

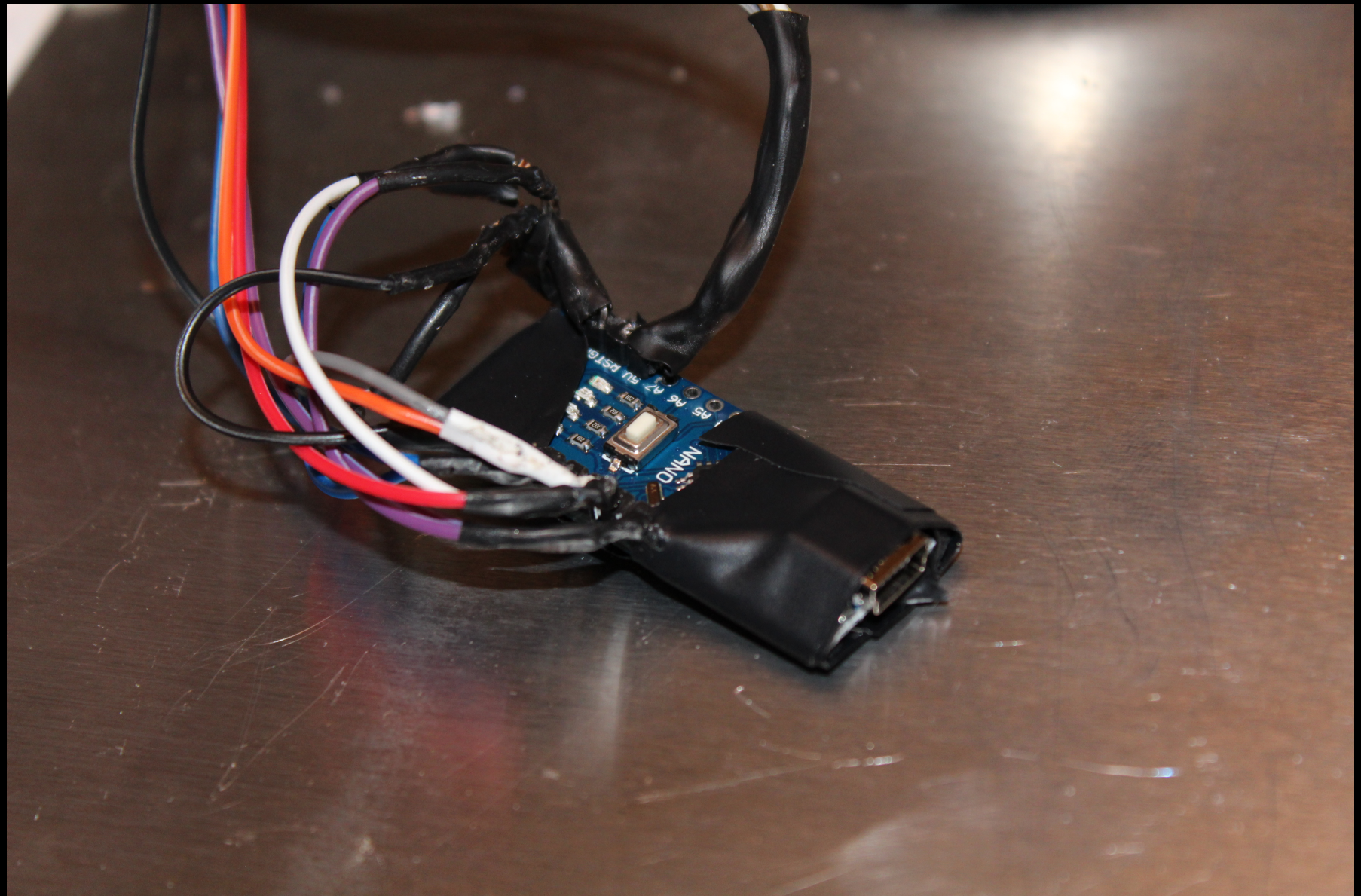


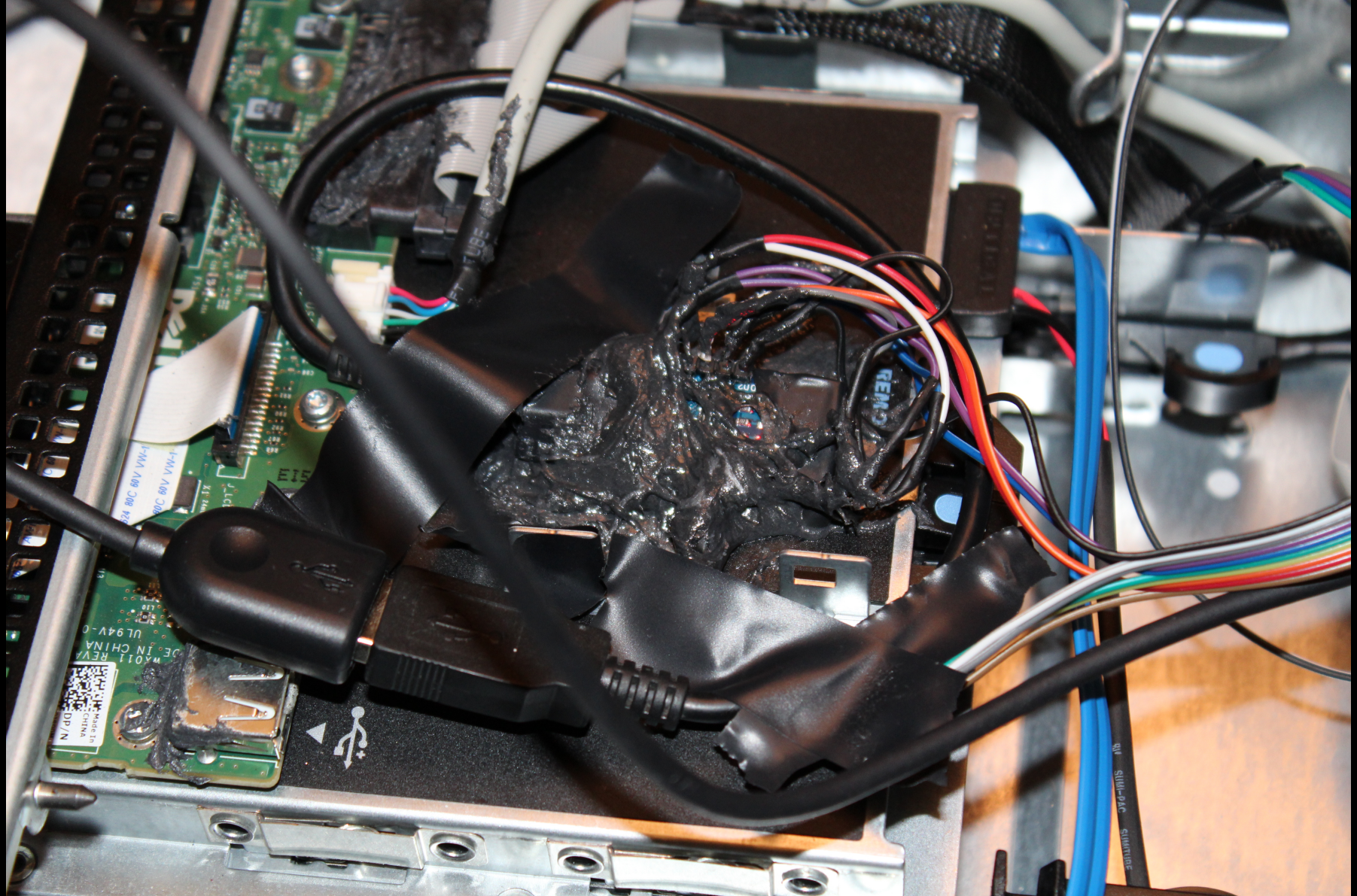

RISER 2
SafeNet
Model:
Part:
Serial#:
5A125VAC-3A250VAC
N.O
N.C
C
de: 0103
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
20130910
C US
N11276
CE
RoHS
COMPLIANT
인증번호:
KCC-REM-SFN-VBD-05
B450551
214-009373-003-L








NANO



https://github.com/lavabit/boobietraps


LOCTITE
SUPER GLUE
WARNING!
BONDS SKIN IN SECONDS.
IRRITANT. See back panel.
45209
.18 OZ
(5g)
1750635
ULTRA LIQUID CONTROL.


MG Chemicals
RED
INSULATING
VARNISH
CAT. NO.
4228-55ML
CONTENTS
55 ml, 2 fl.oz.
DANGER
POISON. FLAMMABLE.



```
LUKS header information for /dev/sdb

Version:        1
Cipher name:    aes
Cipher mode:    xts-plain64
Hash spec:      sha256
Payload offset: 4096
MK bits:        256
MK digest:      67 21 62 31 87 8b cf 12 9c 44 4c 86 6c f8 70 fb b5 df dc 30
MK salt:        6e e6 9d b8 cd de 56 67 cb c1 b4 87 15 5a 1c 0a
                82 0c 73 7a c5 bd f8 c7 25 e5 77 bb 98 e1 ee b3
MK iterations:  172000
UUID:           0ee98914-91a0-4376-b7f9-0f9692f91d61

Key Slot 0: DISABLED
Key Slot 1: ENABLED
        Iterations:             1280000
        Salt:                   52 3b 73 71 3e b7 bb 11 0a d2 46 69 7b f2 4f b4
                                6d 2d 03 17 03 65 3d 79 06 e1 3e 99 93 27 cd 1d
        Key material offset:    264
        AF stripes:             4000
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

https://github.com/hephaest0s/usbkill


It's Birthday!