

ALSO AKADEEMIA

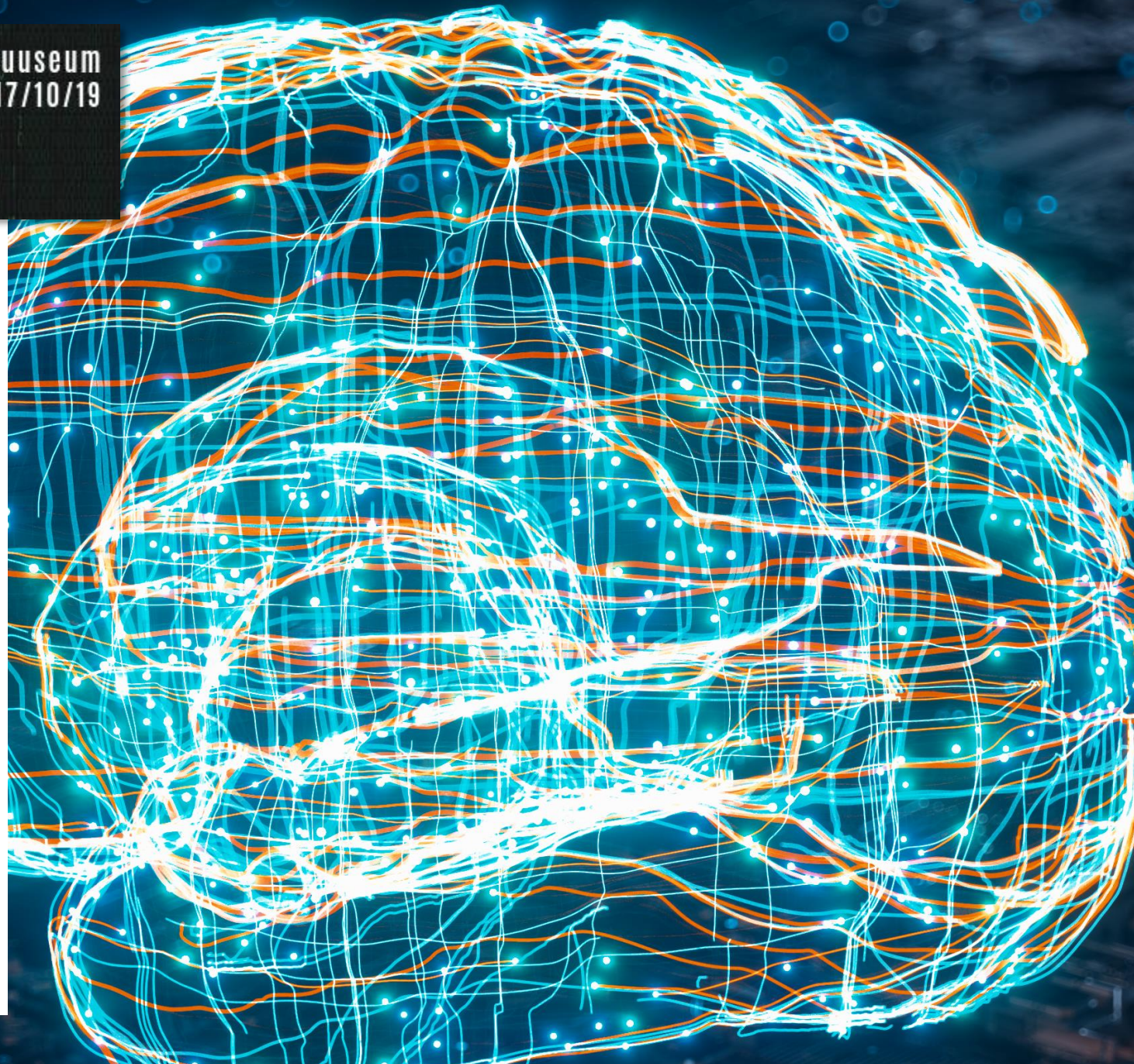
SECURITY DAY  REGISTREERU NÜÜD!

@Filmimuuseum
17/10/19

Securing the Office of the Future with Self- Healing Solutions

Managing end user experiences with
self-healing systems and proactive,
actionable data.

Riku Reimaa
Technical Pre-sales and Technology Evangelism
GWE, Finland and the Baltics
riku@hp.com







Collaboration, innovation, flexibility
and the future of work





PROGRESS

FROM

PRODUCT TO EXPERIENCE

Consumers sought out individual products, consuming them. Focus was on the product itself.

- The Product Age

Consumers show preference for the experience the product will give, or the experience of acquiring that product.

- The Experience Age



INNOVATION, COLLABORATION, SECURITY, MANAGEABILITY





WORKPLACES ARE MORE VULNERABLE





EVERY PC PURCHASE IS A
SECURITY DECISION

■ PROACTIVE MANAGEMENT

Enforce security policies and actively monitor and respond to malicious activity

HP DaaS Proactive Security - NEW

Powered by HP TechPulse

■ RESILIENT HARDWARE

Hardware that can self monitor and self heal if an attack gets in



Sure Start



Sure Recover

■ LAYERS OF PROTECTION

Proactively prevent threats – below, in, and above the OS



Sure Click



Sure Sense



Sure Run



Sure View

DEFENSE IN DEPTH:
WORLD'S MOST SECURE AND MANAGEABLE PCs²⁴



Self-healing systems



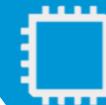
MANAGEMENT AND COMPLIANCE

Modern management
Security compliance



OPERATING SYSTEM AND APPS

Protect key operating system
processes
Secure browsing and self-service
recovery



DEVICE DRIVERS AND FIRMWARE

BIOS and drivers



HARDWARE ENFORCED SECURITY

HP Endpoint Security Controller



SHARE



Michael Archambault
@writingmichaela

POSTED ON
27:18 - 11:50AM

COMPUTING

'LoJax' rootkit malware infects
infects UEFI, a core computer
interface



LoJax UEFI Rootkit Used in Cyberespionage

October 01, 2018



Security researchers from ESET came across a Unified

September 27, 2018

The lowdown on LoJax: Researchers detect a UEFI rootkit in the wild

[Bradley Barth](#) Senior Reporter

Follow @bbb1216bbb



The Russian APT group [Sednit](#) (aka [Fancy Bear](#) and [APT28](#)) is strongly suspected to be the culprit behind a new rootkit malware program that can survive on an infected machine even if the operating system is reinstalled and the hard drive is replaced.

[ESET](#) researchers who discovered the rootkit say this is the first time researchers successfully detected an in-the-wild UEFI rootkit that exploits the Unified



as well as

Related Posts

- Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes
- ESLint Submodules Hacked: Devs Advised to Enable Layered Authentication, Renew Tokens
- Check Your Accounts: Timehop, Macy's, Bloomingdale's, Domain Factory Announce Breach
- PyRoMinelot Targets, Infects, and Spreads to Vulnerable IoT Devices

Fancy Bear LoJax documented

The exploit can be used to patch an



By Charlie Osborne for Zero Day | September 27, 2018 -- 10:03 GMT (11:03 BST)

in the wild



enable or ren
disable BIOS memory opt
Mode to remo
to select Ac

enable or ren
disable BIOS memory opt
Mode to remo
to select Ac

noittemroT

00000000

h dump

ATA F

NOXX

STADIUM

Legacy change management processes are not keeping pace with the rate of change.

A problem has been detected and windows has been shut do
to your computer.
The problem seems to be caused by the following file: at
If this is the first time you've seen this stop error SC
restart your computer. If this screen appears again, fol
these steps:
The device driver got stuck in an infinite loop. This is
problem with the device itself or with the device driver
hardware incorrectly.
Please check with your hardware device vendor for any dr
Technical Information:
*** STOP: 0x000000EA (0x890C2020, 0x00000000, 0x00000000, 0x00000000)
Beginning dump of physical memory

A problem has been detected and windows has been shut do
to your computer.
The problem seems to be caused by the following file: at
If this is the first time you've seen this stop error SC
restart your computer. If this screen appears again, fol
these steps:
The device driver got stuck in an infinite loop. This is
problem with the device itself or with the device driver
hardware incorrectly.
Please check with your hardware device vendor for any dr
Technical Information:
*** STOP: 0x000000EA (0x890C2020, 0x00000000, 0x00000000, 0x00000000)
Beginning dump of physical memory

World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records
(updated 1st Feb 2019)

Colour YEAR DATA SENSITIVITY Filter

2019

2018

DETECT | PROTECT | RECOVER



Nine out of Ten
(91%) visual hacking
attempts succeed.

Average based on global trials conducted by Ponemon Institute during the "Visual Hacking Experiment," 2015, and the "Global Visual Hacking Experiment," 2016, both sponsored by 3M

The greatest security
threats are untrained
users and poor
browsing habits.

PWC "Strengthening digital society against cyber shocks: key findings from The Global State of Information Security® Survey 2018"

The majority of IT
executives see
security as a high
priority.

IDC, 2016 Commercial Survey: PC Results, Doc # US41101516,
March 2016



Security and Manageability across Client and Print Solutions

Managing and measuring experiences with proactive analytics

Powered by HP TechPulse





- Dashboard
- Companies
- Incidents
- Devices
- Users
- Reports
- Logs
- Settings
- Help & Support
- EMM Tool
- Microsoft Telemetry

DEVICES HEALTH

3

BATTERY REPLACEMENT

Number of batteries that require replacement

0

DISK REPLACEMENT

Number of disks that require replacement

0

DISK CAPACITY

Number of disks near maximum capacity

0

THERMAL GRADING

Number of devices that have bad thermal grade

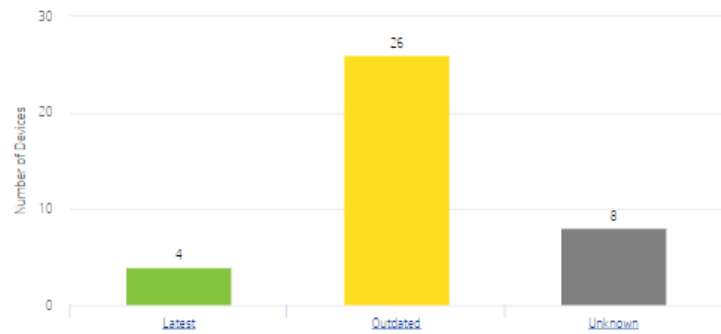


BUSINESS REVIEW

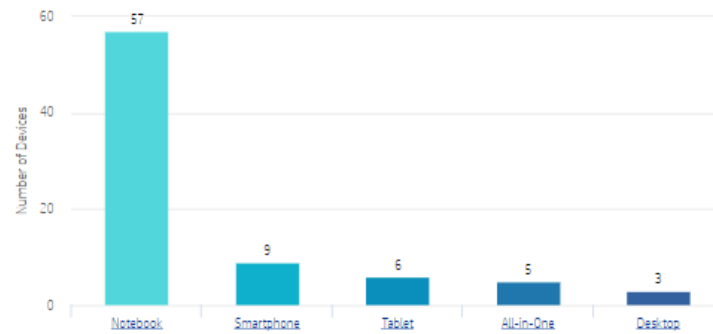
Generate a summary report for the months, reports and companies of your choice.

GENERATE REPORT

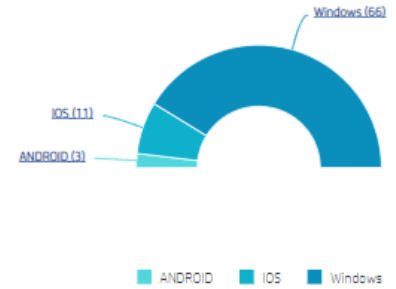
WINDOWS 10 VERSION STATUS



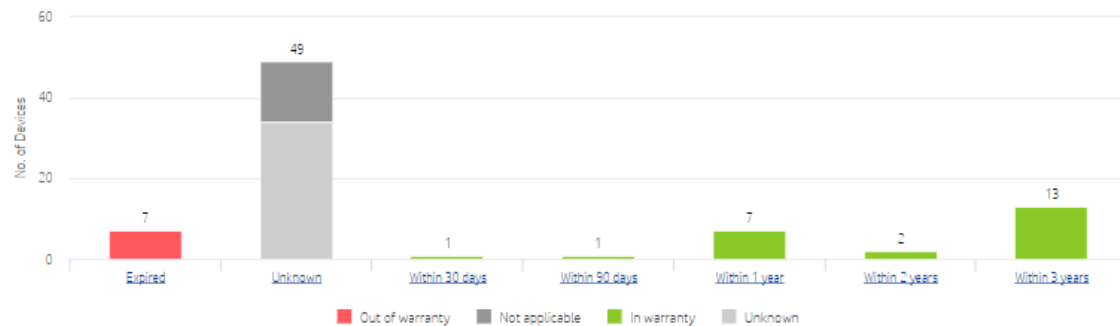
DEVICES BY TYPE



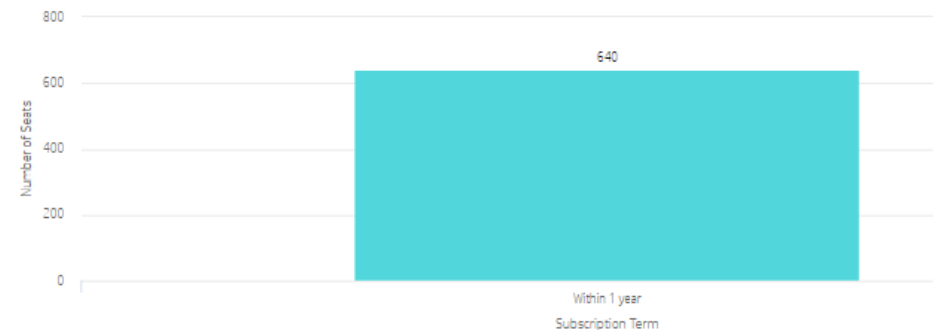
DEVICES BY OS



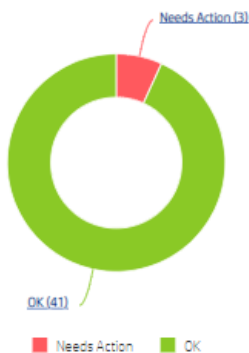
WARRANTY EXPIRATION



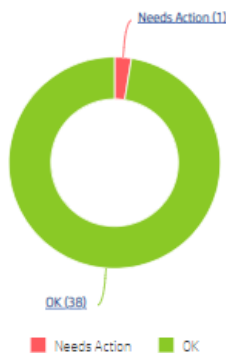
SUBSCRIPTION EXPIRATION



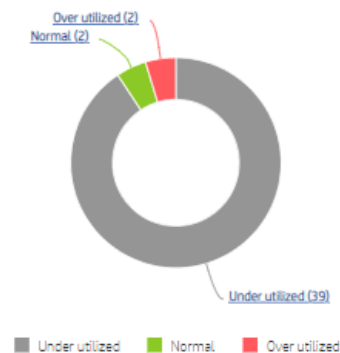
BATTERY REPLACEMENT SUMMARY



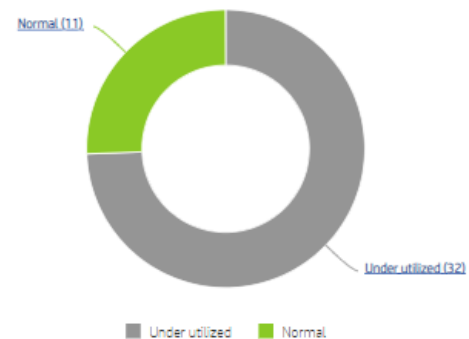
DISK REPLACEMENT SUMMARY



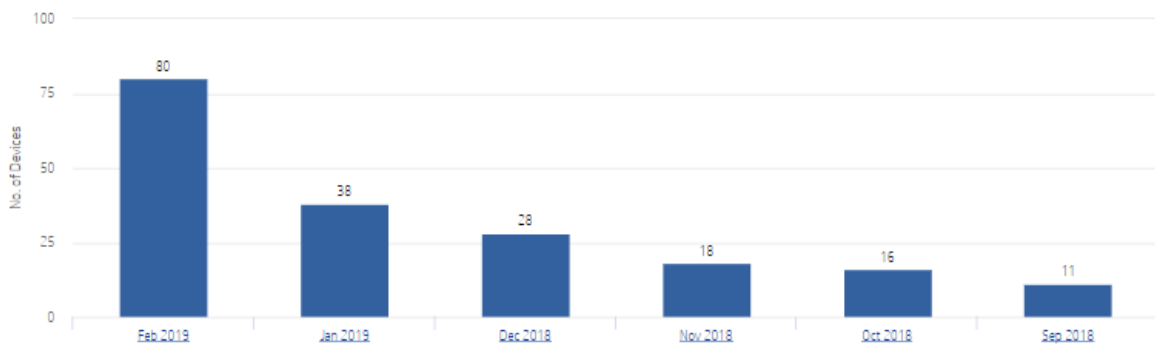
CPU UTILIZATION



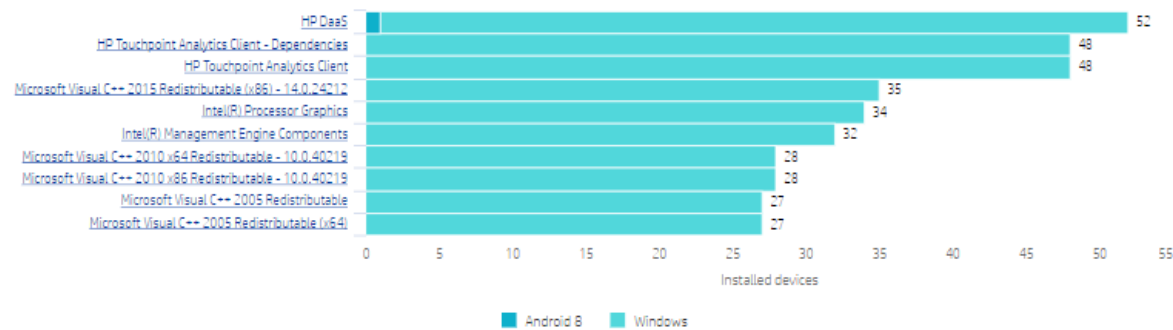
MEMORY UTILIZATION



HARDWARE INVENTORY



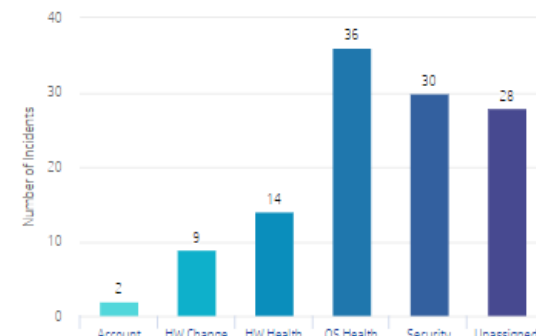
SOFTWARE INVENTORY (TOP 10)



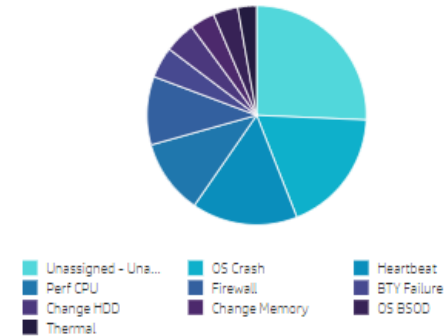
OPEN INCIDENTS



ALL INCIDENTS



TOP 10 INCIDENTS



Multi-platform support across devices



HP DaaS is available on several platforms.

Please select which one you would like to download and install.

HP TechPulse Android Application

Version 2.1.83.0

Released on April 25, 2019



HP TechPulse macOS Application

Version 1.14.469

Released on July 24, 2019

DOWNLOAD

HP TechPulse Windows Application

Version 3.19.160

Released on May 10, 2019

Expires on February 03, 2020

[Download Policy File](#)

[VIEW MORE VERSIONS](#)

DOWNLOAD

HP TechPulse Incident Integration

Version 1.0.2

Released on May 30, 2019

DOWNLOAD

HP Sure Click Advanced Security Application

Version 4.1.5.1297

Released on March 30, 2019

DOWNLOAD



HP TechPulse

- Multi-platform view of device performance and health
- Database of over 40 million devices being leveraged for machine learning and AI –driven analytics
- Value-add services for security related reporting
- Simple and easy onboarding



keep reinventing