

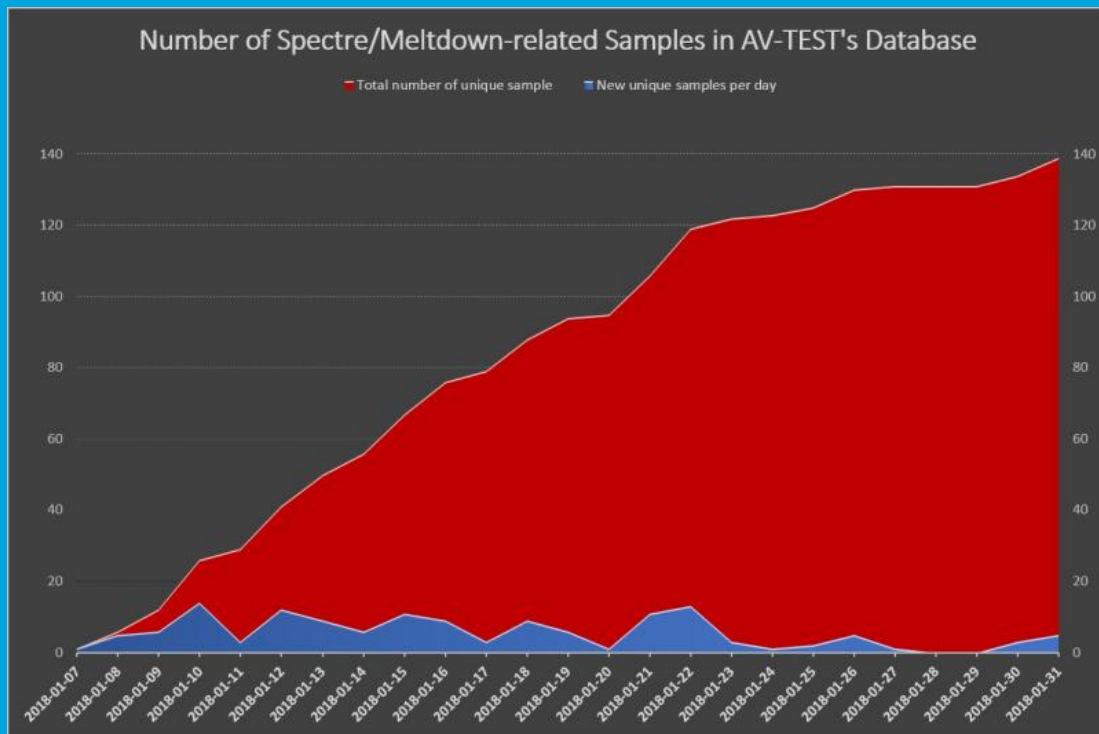


Security Newsletter

5 February 2018

[Subscribe to this newsletter](#)

Spectre and Meltdown flaws being exploited by more than 100 strains of malware



Researchers have discovered more than 130 malware samples designed to exploit the recently disclosed Spectre and Meltdown CPU vulnerabilities. While a majority of the samples appear to be in the testing phase, we could soon start seeing attacks.

The Meltdown and Spectre attack methods allow malicious applications to bypass memory isolation mechanisms and access passwords, photos, documents, emails, and other sensitive data. Shortly after Spectre and Meltdown were disclosed on January 3, experts warned that we could soon see remote attacks, especially since a JavaScript-based proof-of-concept (PoC) exploit for Spectre had been made available.

"The most likely attack method regarding Spectre and Meltdown will be via web browsers and their integrated scripting engines. So I'd recommend to upgrade to the latest available versions as soon as possible," he said, adding that closing the browser and shutting down the PC when it's not in use would also reduce the risk.

However, patching against variant 2 of the Spectre vulnerability has proven to be particularly difficult, due to it being related to a fundamental feature of modern CPUs, specifically their use of Branch Prediction and Speculative Execution to accelerate the rate at which they operate. "Which is why, in addition to establishing an aggressive and proactive patch-and-replace protocol, it is essential that organizations have layers of security in place designed to detect malicious activity and malware, and to protect vulnerable systems."

[Read More](#)[Even More](#)

Crooks Created 28 Fake Ad Agencies to Disguise Massive Malvertising Campaign



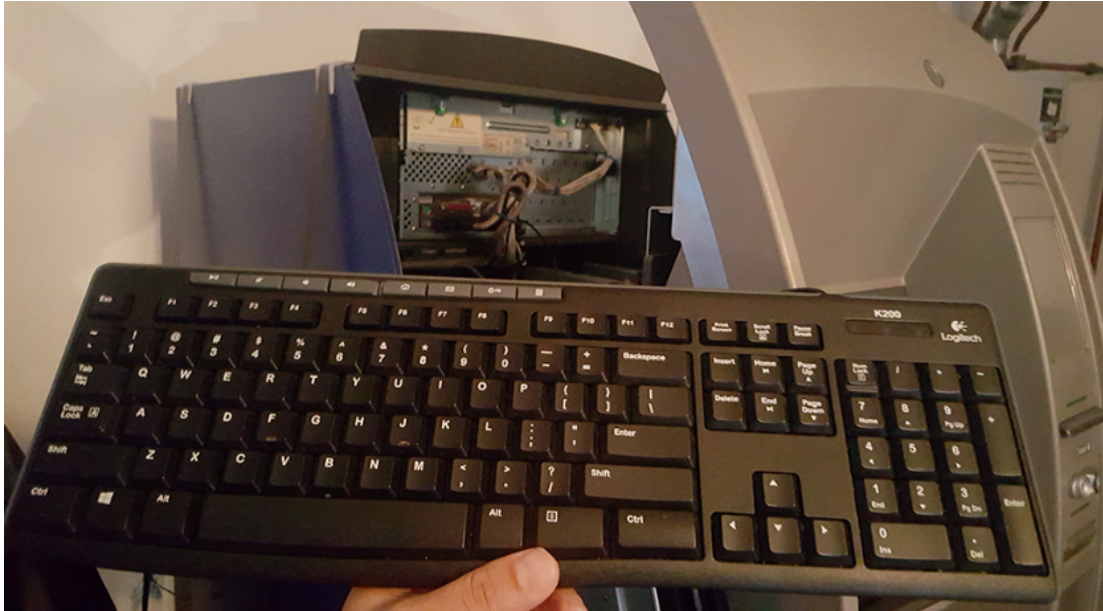
A group of cyber-criminals created 28 fake ad agencies and bought over 1 billion ad views in 2017, which they used to deliver malicious ads that redirected unsuspecting users to tech support scams or sneaky pages peddling malware-laden software updates or software installers. The entire operation —codenamed Zirconium— appears to have started in February 2017, when the group started creating the fake ad agencies which later bought ad views from larger ad platforms. These fake ad agencies each had individual websites and even LinkedIn profiles for their fake CEOs. Their sole purpose was to interface with larger advertising platforms, appearing as legitimate businesses.

The fake ad agencies would buy ads displayed on legitimate sites via these ad platforms. These ads would allow the Zirconium group to run JavaScript code that executed a "forced redirect," effectively hijacking visitors off the original site to an intermediary domain. This intermediary domain would fingerprint and classify incoming traffic, then redirect the user to another domain, also operated by Zirconium. Crooks would use this third domain as an affiliate traffic jump-off point, allowing others to buy the traffic they hijacked from legitimate sites. In many cases, users were redirected to pages offering fake (malware-laced) Flash updates, websites offering (malware-infested) software installers, tech support scams, or other scareware pages.

Dangu believes that improved browser security features now make most exploit kits ineffective. In addition, the decision from most browser makers to change Flash into a disabled state or click-to-run policy have also contributed to the demise of classic malvertising+exploit kit campaigns. Chrome 64, released earlier this week, blocks the forced redirect technique (also known as tab-under) used by the Zirconium group.

[Read More](#)

First 'Jackpotting' Attacks Hit U.S. ATMs



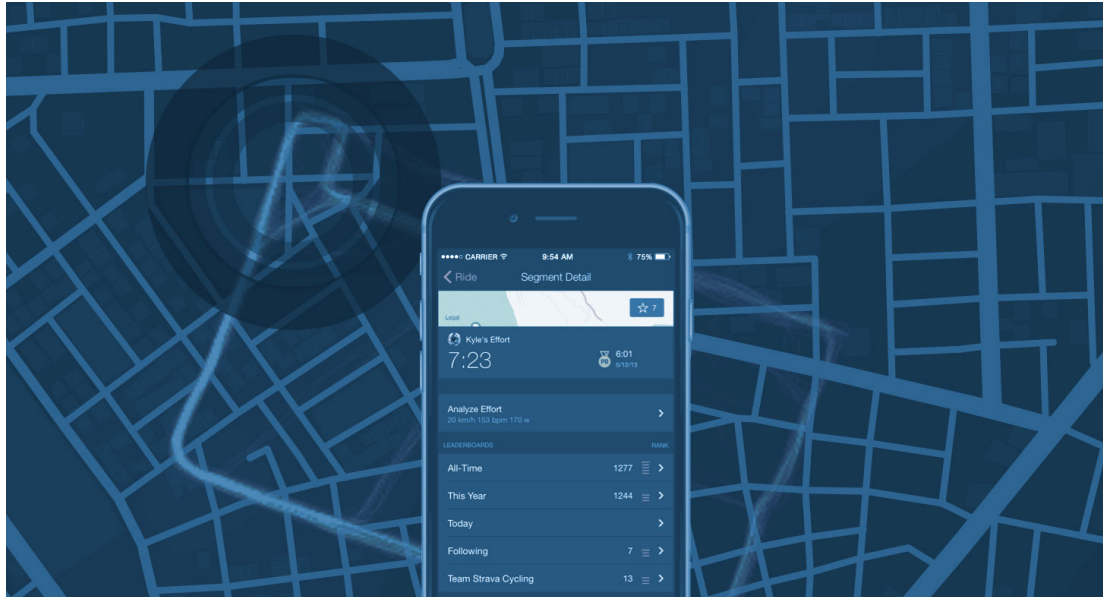
ATM “jackpotting” — a sophisticated crime in which thieves install malicious software and/or hardware at ATMs that forces the machines to spit out huge volumes of cash on demand — has long been a threat for banks in Europe and Asia, yet these attacks somehow have eluded U.S. ATM operators. But all that changed this week after the U.S. Secret Service quietly began warning financial institutions that jackpotting attacks have now been spotted targeting cash machines here in the United States.

To carry out a jackpotting attack, thieves first must gain physical access to the cash machine. From there they can use malware or specialized electronics — often a combination of both — to control the operations of the ATM. “The targeted stand-alone ATMs are routinely located in pharmacies, big box retailers, and drive-thru ATMs,” reads a confidential Secret Service alert sent to multiple financial institutions and obtained by KrebsOnSecurity. “During previous attacks, fraudsters dressed as ATM technicians and attached a laptop computer with a mirror image of the ATMs operating system along with a mobile device to the targeted ATM.”

Regalado says the crime gangs typically responsible for these attacks deploy “money mules” to conduct the attacks and siphon cash from ATMs. The term refers to low-level operators within a criminal organization who are assigned high-risk jobs, such as installing ATM skimmers and otherwise physically tampering with cash machines. The Secret Service alert says ATMs still running on Windows XP are particularly vulnerable, and it urged ATM operators to update to a version of Windows 7 to defeat this specific type of attack.

[Read More](#)[Even More](#)

Strava exercise app maps military sites, reveals where spies jog



In November, exercise-tracking app Strava published a “heatmap” of user activity which it cheerily boasted comprised a billion activities, three trillion lat-long points, 13 trillion rasterized pixels and 10 TB of input data. Several people and media institutions have revealed military bases around the world using the heatmap.

Strava's explanation of how it made the Heatmap says it excluded data that users asked to be kept private. The service allows users to create multiple “privacy zones” with a radius of up to 1 km. When users enter such the zones, their digital tracks disappear in order to make it harder to figure out where they live or work. Data revealing the location of sensitive facilities, or the habits of military personnel, would therefore have been excluded if users had employed Strava's privacy settings.

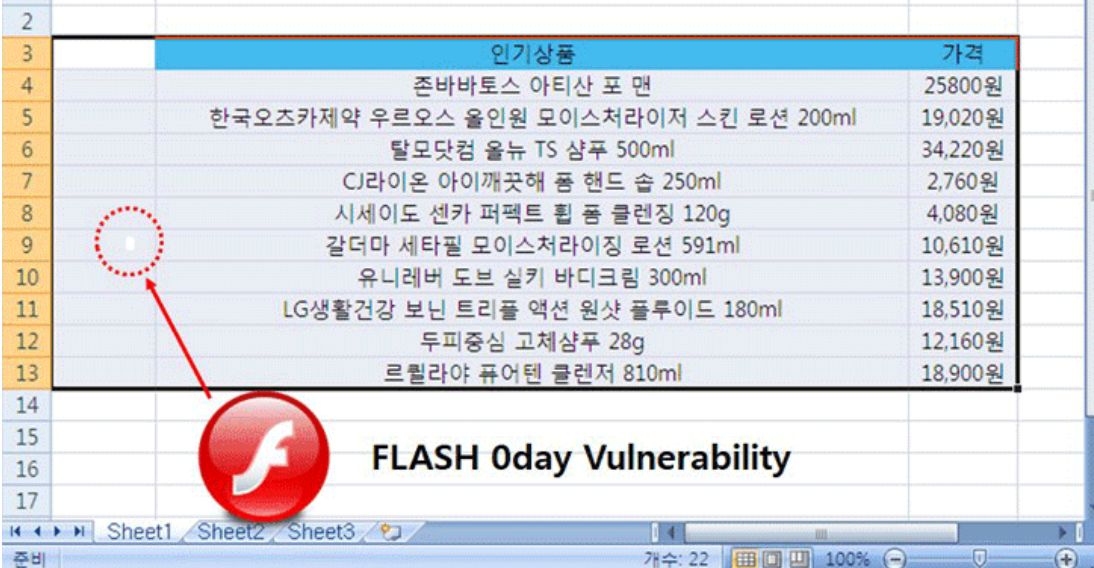
However, as Ruser later tweeted, the location of bases isn't the only concern: the ability to establish “pattern of life” information also makes the Heatmap a serious source of risk – mainly because people weren't keeping their information private. It also, by the way, possible to extract people's names, profile pictures, and heart rates from Strava's backend.

Olejnuk said at the least, someone should have conducted a privacy impact statement before pressing “publish” on the dataset. He told The Register in an email: “This highlights the challenges of location data anonymisation, and how mass datasets reveal unexpected patterns. Organisations should carefully consider consequences on multiple levels prior to publishing private data.

[Read More](#)

[Even More](#)

Attackers Exploiting Unpatched Flaw in Flash



인기상품	가격
존바바토스 아티산 포 먼	25800원
한국오즈카제약 우르오스 올인원 모이스처라이저 스킨 로션 200ml	19,020원
탈모닷컴 올뉴 TS 샴푸 500ml	34,220원
CJ라이온 아이깨끗해 폼 핸드 슝 250ml	2,760원
시세이도 센카 퍼펙트 토탈 폼 클렌징 120g	4,080원
갈더마 세타필 모이스처라이징 로션 591ml	10,610원
유니레버 도브 실키 바디크림 300ml	13,900원
LG생활건강 보닌 트리플 액션 원샷 플루이드 180ml	18,510원
두피중심 고체샴푸 28g	12,160원
르엘라야 퓨어텐 클렌저 810ml	18,900원

FLASH 0day Vulnerability

Adobe warned on Thursday that attackers are exploiting a previously unknown security hole in its Flash Player software to break into Microsoft Windows computers. Adobe said it plans to issue a fix for the flaw in the next few days, but now might be a good time to check your exposure to this still-ubiquitous program and harden your defenses. Successful exploitation could allow an attacker to take control of the affected system.

The software company warns that an exploit for the flaw is being used in the wild, and that so far the attacks leverage Microsoft Office documents with embedded malicious Flash content. Adobe said it plans to address this vulnerability in a release planned for the week of February 5.

For readers still unwilling to cut the Flash cord, there are half-measures that work almost as well. Fortunately, disabling Flash in Chrome is simple enough. Paste "chrome://settings/content" into a Chrome browser bar and then select "Flash" from the list of items. By default it should be set to "Ask first" before running Flash, although users also can disable Flash entirely here or whitelist and blacklist specific sites. By default, Mozilla Firefox on Windows computers with Flash installed runs Flash in a "protected mode," which prompts the user to decide if they want to enable the plugin before Flash content runs on a Web site.

[Read More](#)

[Even More](#)

Breach-Proofing Your Data in a GDPR World



The massive data breaches that have hit the headlines in recent years, including Yahoo, Verizon, and particularly Equifax, have taken a toll on breach victims, consumers, and corporations. This year, breaches could be even more costly for companies once the European Union's General Data Protection Regulation (GDPR) rules are in place come May 25.

Organizations are under the gun to get systems in place now to ensure that they are in compliance with the regulations, before it's too late. Here are six key measures for enterprises to prioritize over the next few months: 1) Protect data beyond your perimeter, expanding use of enterprise security controls is crucial, but end-to-end data protection is one of the most potent safeguards. 2) Make privacy awareness mandatory, by requiring every employee to participate in cybersecurity awareness training and conducting training on an ongoing basis. 3) Ensure secure transmission of data in the cloud. 4) Check the terms and conditions, nearly 40% of cloud services provide terms and conditions that lack specifics around data ownership. 5) Know your data well, what information is being collected, who's collecting it, and who's sharing it throughout the organization. 6) Follow your data, especially if it crosses geopolitical boundaries.

[Read More](#)[Even More](#)

AutoSploit: Automated Hacking Tool Set to Wreak Havoc or a Tempest in a Teapot?



Python code has emerged that automatically searches for vulnerable devices online using Shodan.io – and then uses Metasploit's database of exploits to potentially hijack the computers and gadgets. You set this script running, it crawls the internet looking for machines that are possibly vulnerable to attack – typically due to unpatched security bugs – and automatically takes over them for you. No super-l33t skills required.

Metasploit is an open-source penetration testing tool: it is a database of snippets of code that exploit security flaws in software and other products to extract information from systems, or open a remote control panel to the devices so they can be commanded from afar. Shodan allows you to search for public-internet-facing computers, servers, industrial equipment, webcams, and other devices, revealing their open ports and potentially exploitable services.

Just how dangerous is this? Opinions are varied. "[AutoSploit] makes being a script kiddie infinitely easier," comments Chris Morales, head of security analytics at Vectra Networks. "It is combining a whole set of automated tools for identifying exposed hosts and then executing exploits. Where I think this will have the most dramatic effect, and what scares me most, is with IoT. I'm predicting a rash of new IoT DOS, cryptocurrency mining, and general debauchery." "The kids are not more dangerous," he says. "They already were dangerous. We've simply given them a newer, simpler, shinier way to exploit everything that's broken. Maybe we should fix the ROOT problem."

[Read More](#)[Read More](#)

Cutting room floor

- [First Malicious Chrome Extensions Detected Using Session Replay Scripts](#)
- [Poor Visibility, Weak Passwords Compromise Active Directory](#)
- [Data Encryption: 4 Common Pitfalls](#)
- [Most Threatening DNS Security Risks And How To Avoid Them](#)
- [Mozilla Fixes Severe Flaw in Firefox UI That Leads to Remote Code Execution](#)
- [Remotely Exploitable Vulnerability Could Impact 300,000 Oracle PoS Systems](#)
- [Nasty botnet uses WannaCry exploit to mine cryptocurrency from your servers](#)
- ['Panty Buster' Toy Left Private Sex Lives Of 50,000 Exposed](#)
- [Microsoft Drops the Hammer on Coercive Registry Cleaners & System Optimizers](#)
- [What's Riding on 5G Security? The Internet of Everything](#)
- [Hard-coded Password Lets Attackers Bypass Lenovo's Fingerprint Scanner](#)

#Tech and #Tools

- [DCShadow explained: A technical deep dive into the latest AD attack technique](#)
- [My Blog Now Has a Content Security Policy - Here's How I've Done It](#)
- [The EMET Attack Surface Reduction Replacement in Windows 10 RS3: The Good, the Bad, and the Ugly](#)
- [The Challenges Of Securing And Protecting Containers During Runtime](#)
- [Internet of dildos: a long way to a vibrant future](#)
- [LuLu: Free open-source macOS firewall blocking unknown outgoing connections](#)
- [Web Application Firewall \(WAF\) Evasion Techniques](#)
- <https://github.com/wetw0rk/Sickle>
- [Hacking With Go: Packet Crafting and Manipulation in Golang Pt 1](#)
- [Honey Buckets: Find out who is snooping through your Amazon S3 buckets.](#)

This content was created by [Kindred Group Security](#). Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at <https://news.infosecgur.us>

If you no longer wish to receive this newsletter, you can [unsubscribe from this list](#).

