NewsBytes – January, 2019

Your Monthly News Digest

$: whoami

Nishant Grover

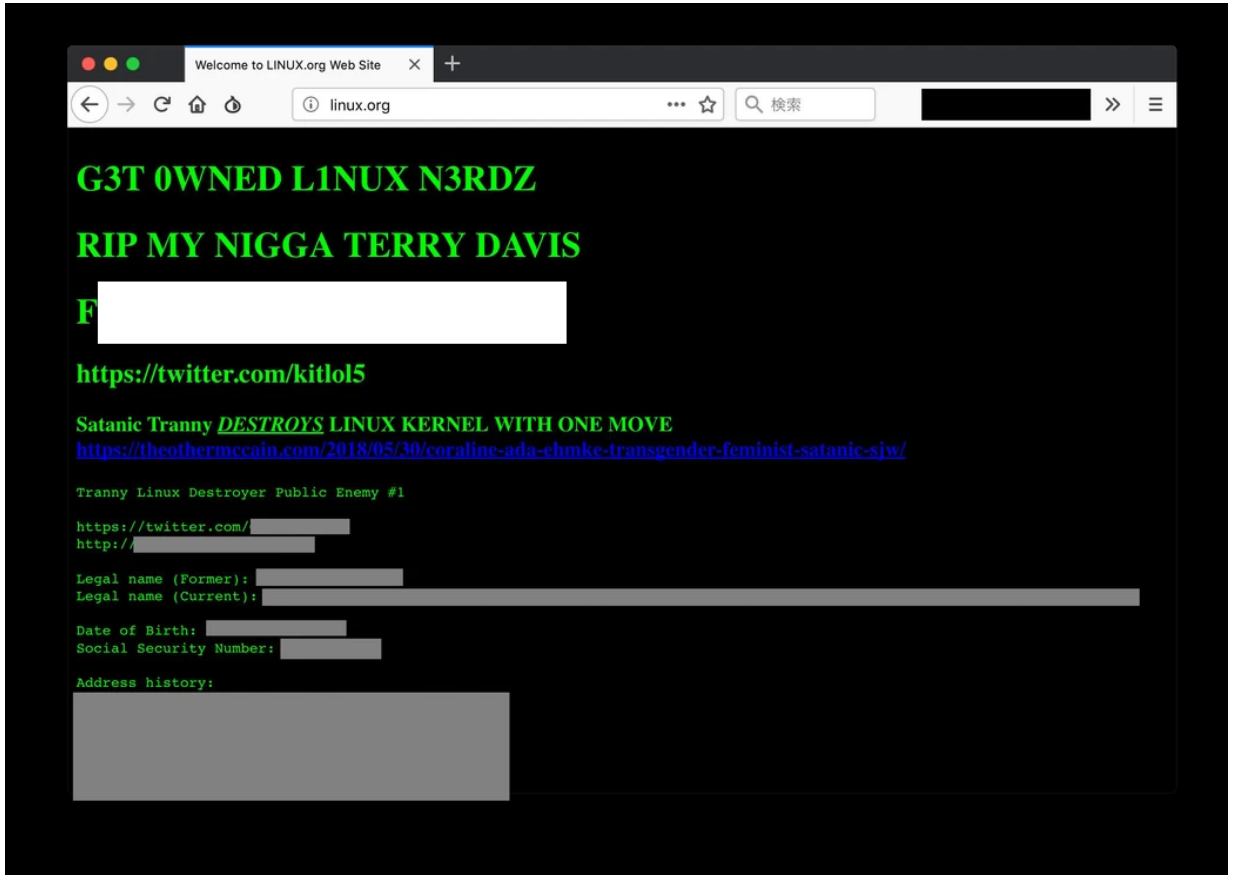
Interest: Incident Response, Scripting, threat hunting

@ngrovyer

Linux.org DNS Hijacked

Dec 7

- Domain registration Account hijacked with Credentials guessing
- Several domains including linuxonline.com, linuxhq.com, linux.org as well as McLagan's personal website were hijacked.
- Actual linux.org servers were untouched and no data was leaked.



Zero-Day Flash Player Vulnerability Fixed After Being Exploited In the Wild

Dec 10

- Adobe has patched critical zero-day Flash Player vulnerability.
- Allow an attacker to execute arbitrary commands.
- Several researchers reported this critical use after free vulnerability (CVE-2018-15982) to Adobe.
- However, Adobe confirmed the wild exploits of this vulnerability.

Another Important Vulnerability Also Patched

- Adobe also fixed an important security vulnerability in Flash Player.
- This Insecure Library Loading (DLL hijacking) vulnerability (CVE-2018-15983) could lead to privilege escalation.

Eastern European Banks hacked by Sneaky devices

Dec 10

Kaspersky Lab reports that its specialists were asked to investigate a series of cybertheft incidents.

- In each case, they discovered an unknown device connected to a company's local network. These consisted of either a netbook or similar cheap laptop, a Raspberry Pi, or a Bash Bunny—a special tool intended for use in penetration testing that looks like a flash drive.
- Once a device was in place, remote access was achieved via a built-in or USB-connected GPRS/3G/LTE modem.
- Kaspersky has given these hacks the codename "DarkVishnya," and said they took place through 2017 and 2018. It estimates the damage caused to be in the tens of millions of dollars.

Microsoft patches nine critical bugs as part of December Patch Tuesday roundup

Dec 11

- The vulnerability (CVE-2018-8611) is an elevation-of-privilege (EoP) bug that affects Windows 7 through Server 2019. It has a CVSS rating of seven, classifying it as a high-severity flaw.
- An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode.

Microsoft patches nine critical bugs as part of December Patch Tuesday roundup (Cont)

Dec 11(Continue)

Another noteworthy remote code-execution bug CVE-2018-8634 (rated important) impacts Microsoft's text-to-speech engine.

- First, newer functionalities like text-to-speech have a somewhat unknown attack surface,
- Microsoft doesn't state a sample exploit scenario, but since generating speech requires an HTTP POST request to the speech service, it's possible this could be remotely accessible if your application is network facing.

In addition to the zero-day bug, Microsoft patched nine critical vulnerabilities and 30 flaws rated important, from Internet Explorer, Edge, ChackraCore, Microsoft Windows, Office and Microsoft Office Services and Web Apps, and the .NET Framework.

A bug left your Microsoft account wide open to complete takeover

Dec 11

- Bug bounty hunter Sahad Nk (Kerala based Techie) recently uncovered a series of vulnerabilities that left Microsoft users' accounts, and received unknown amount of Bounty
- Nk discovered that he was able to take over the Microsoft subdomain, http://success.office.com, because it wasn't properly configured.
- Azure web app that pointed to the domain's CNAME record, which maps domain aliases and subdomains to the main domain
- Microsoft Office, Outlook, Store, and Sway apps send authenticated login tokens to the http://success.office.com subdomain. When a user logs in to Microsoft Live, login.live.com, the login token would leak over to the server controlled by Nk. He would then just have to send over an email to the user asking them to click a link, which would provide Nk with a valid session token to their account.

Equifax Hack Lasted for 76 Days, Compromised 148 Million People

Dec 12

- Equifax hack was entirely preventable, had they have patched their systems in 2 months before hackers actually started accessing their networks
- Equifax didn't have clear "lines of authority" for ensuring digital security and failed to patch its systems when a vulnerability was publicly disclosed in 2017.
- The device used to monitor [the vulnerable server's] network traffic had been inactive for 19 months due to an expired security certificate. It took another two months for Equifax to update the expired certificate, at which point staff immediately noticed suspicious web traffic.

Bug allowed full takeover of Samsung user accounts

Dec 12

Samsung awards researcher a $13,300 reward for finding three CSRF issues on its user portal.T

- The first would have allowed an attacker to change profile details
- The second would have allowed an attacker to disable two-factor authentication
- The third would have allowed an attacker to change the user's account security question.

Marriott Data Breach

Dec 13

- Investigators believe hackers working on behalf of China's main intelligence agency are responsible. The Breach went undetected for 4 years!

Jan 04

- The Marriott has now advised that it believes as many as 383 million records (not 500m) were accessed in the data breach.

Jan 10

- It has been reported that Marriott International Inc. is being sued by 176 plaintiffs from all 50 US states
- Plaintiffs' attorneys say Marriott should have discovered the breach during its acquisition of Starwood in 2016.

Facebook, Under Scrutiny, Pays Out Largest Bug Bounty Yet

Dec 13

- And this year Facebook also paid its biggest single bounty ever, $50,000.
- The bug was in Facebook's developer subscription mechanism for notifications on certain types of user activity.
- The researcher found that in certain situations a developer, or attacker, could have manipulated the subscriptions to receive updates that shouldn't have been authorized about certain actions and users.
- For instance, a rogue developer could have gotten regular updates on who liked or commented on a specific post.

Save the Children Foundation duped by hackers into paying out $1 million

Dec 14

- The con artists managed to compromise an employee's email account in order to masquerade as the staff member in question.
- Once access was gained to the account, the hackers behind the scam created a number of false invoices and related documents which described a need to purchase solar panels for health centers located in Pakistan.
- The Connecticut-based charity organization fell for the ruse, conducted in May 2017, and approved the transfer of close to $1 million to an entity in Japan which was used as a front to rake in the proceeds.
- The publication says that Save the Children possessed insurance which covered close to all of the lost funds, and in the end, the charity only lost $112,000.

Facebook Exposed 6.8 Million Users' Photos to Cap Off a Terrible 2018

Dec 14

- For nearly two weeks in September, a bug let third-party developers view the photos of up to 6.8 million Facebook users, whether they'd shared them or not.
- Facebook will eventually alert affected users with a notification, which will send them to a page that details what happened and which apps might have their photos on hand.
- Those permissions are supposed to apply to photos that you share to your timeline.
- Thanks to this bug, developers could also have accessed photos that you shared to other areas of Facebook, including Marketplace and Stories. More alarmingly, they could have accessed any photos that you uploaded to Facebook but chose not to share at all.

Taylor swift's facial recognition scans crowds for stalkers

Dec 15

- Taylor Swift deployed a sneaky facial recognition camera at her May 18 Rose Bowl show.
- Hidden behind a display that showed short videos of rehearsals, the camera fed footage back to Nashville, where a team ran them against a database of known stalkers.

Twitter Fixes Bug That Gives Unauthorized Access to Direct Messages

Dec 15

- A bug affecting the permissions dialog when authorizing certain apps to Twitter leaves direct messages exposed to the third-party without the user ever knowing about it.
- The flaw manifested with apps that require a PIN to complete the authorization process instead of the OAuth token-based procedure; as a result, some permissions such as that to access direct messages, remained hidden to the Twitter user.
- Terence Eden discovered the issue and reported it to Twitter through the HackerOne bug bounty platform. The disclosure earned him a reward of $2,940.

Thousands of Jenkins servers will let anonymous users become admins

Dec 16

Two vulnerabilities discovered and patched over the summer expose Jenkins servers to mass exploitation.

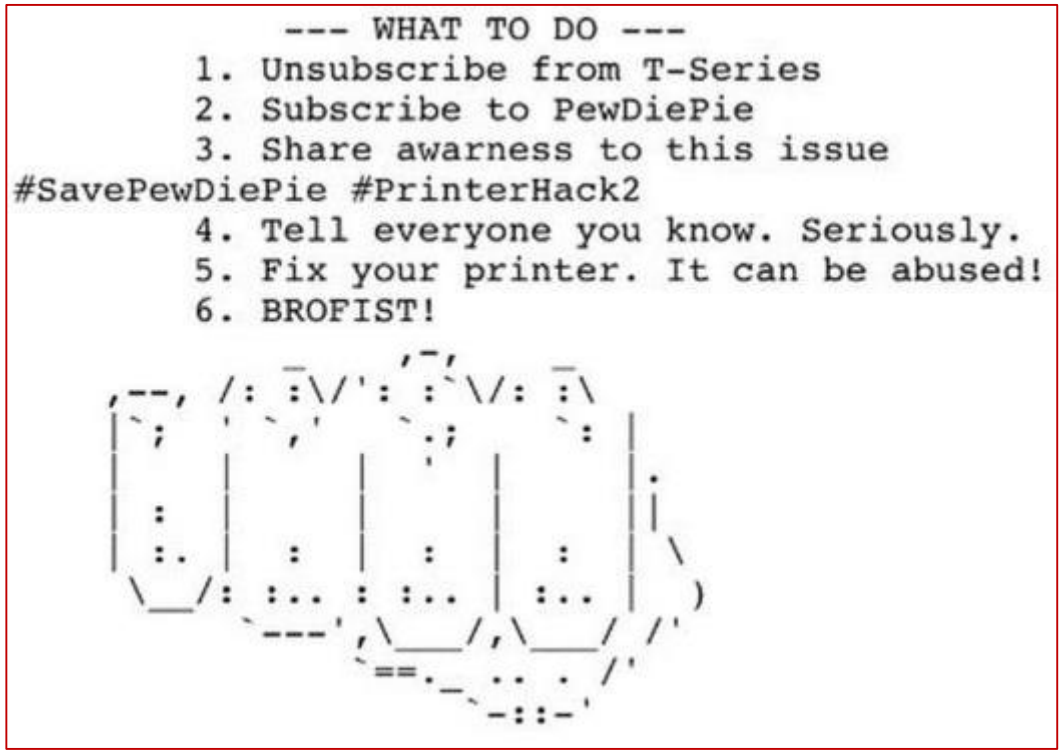
- CyberArk researchers discovered a vulnerability (tracked as CVE-2018-1999001)
- Allows an attacker to provide malformed login credentials that cause servers to move their config.xml file from home directory to another location.
- If an attacker can cause the Jenkins server to crash and restart, or if he waits for the server to restart on its own, the Jenkins server then boots in a default configuration that features no security.

- CyberArk researchers also discovered a second Jenkins vulnerability --CVE-2018-1999043.
- This second bug, they said, allowed an attacker to create ephemeral user records in the server's memory, allowing an attacker a short period when they could authenticate using ghost usernames and credentials.

Thousands of Jenkins servers will let anonymous users become admins

Dec 16

- It is the latest in a series of such attacks, but this time they say they have the power to destroy the machines.
- The stunt was first carried out last month, when one member claimed to have forced about 50,000 printers to create posters supporting his favourite vlogger PewDiePie.
- The latest incident again urges support for the YouTuber, but also calls on victims to improve their security.



53 Bugs in 50 Days: Researchers Fuzz Adobe Reader

Dec 17

- Checkpoint's team 50-day experiment unearthed more than 50 new CVEs in Adobe Reader. An average of one vulnerability per day is "not quite the usual pace for this kind of research," they point out.

- A 50-day timeframe was chosen for the full project: reverse-engineering code, hunting for potential vulnerable libraries, writing harnesses, and running the fuzzer itself.

- For their fuzzer, researchers chose WinAFL, a common Windows fuzzing framework, and targeted Adobe Reader in "the most vanilla experiment we could think of," they explain in a report on the findings.

Twitter warns 'unusual activity' from hackers in China, S Arabia

Dec 18

- Twitter has warned of "unusual activity" from state-sponsored actors based in China and Saudi Arabia after it found a bug that could have revealed the country code of users' phone numbers or if their account was locked.

- The revelation led to Twitter stock dropping nearly 7 per cent on Monday.

- A security researcher found a bug in Twitter's support form two years ago that exposed the country codes of phone numbers attached to users' accounts. At the time, his bug report was closed as it did "not appear to present a significant security risk."

NASA Says Hackers Stole Employee Information

Dec 19

- Hackers downloaded Social Security numbers and other personal information from an unknown number of current and former NASA employees, the agency told workers.
- NASA began investigating the intrusion of its servers on Oct. 23, according to a memo sent Tuesday by Assistant Administrator Bob Gibbs.
- Employees who were hired, transferred or left the agency from July 2006 to October 2018 may have been affected by the hack.
- The agency has about 17,400 civil service employees.

Microsoft Releases Out-of-Band Security Update for Internet Explorer RCE Zero-Day

Dec 19

- This vulnerability has been assigned ID CVE-2018-8653 and was discovered by Google's Threat Analysis Group when they saw the vulnerability being used in targeted attacks.
- A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer
- The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the **context of the current user.**
- This vulnerability can also be used to launch attacks through specially crafted web sites that utilize the exploit code.

Personal details of North Korean defectors stolen after hackers target resettling agency

Dec 28

- Hackers stole the personal information of 997 North Korean defectors after accessing a South Korean resettlement agency's database
- Ministry officials said the breach occurred last month when an employee of the government agency Hanna Foundation opened an email with malware.
- The Hana institution is one of 25 centers that aid approximately 32,000 defectors as they transition to a new life away from the repressive regime.

EU To Offer Almost $1M In Bug Bounties On Open Source Software

Dec 30

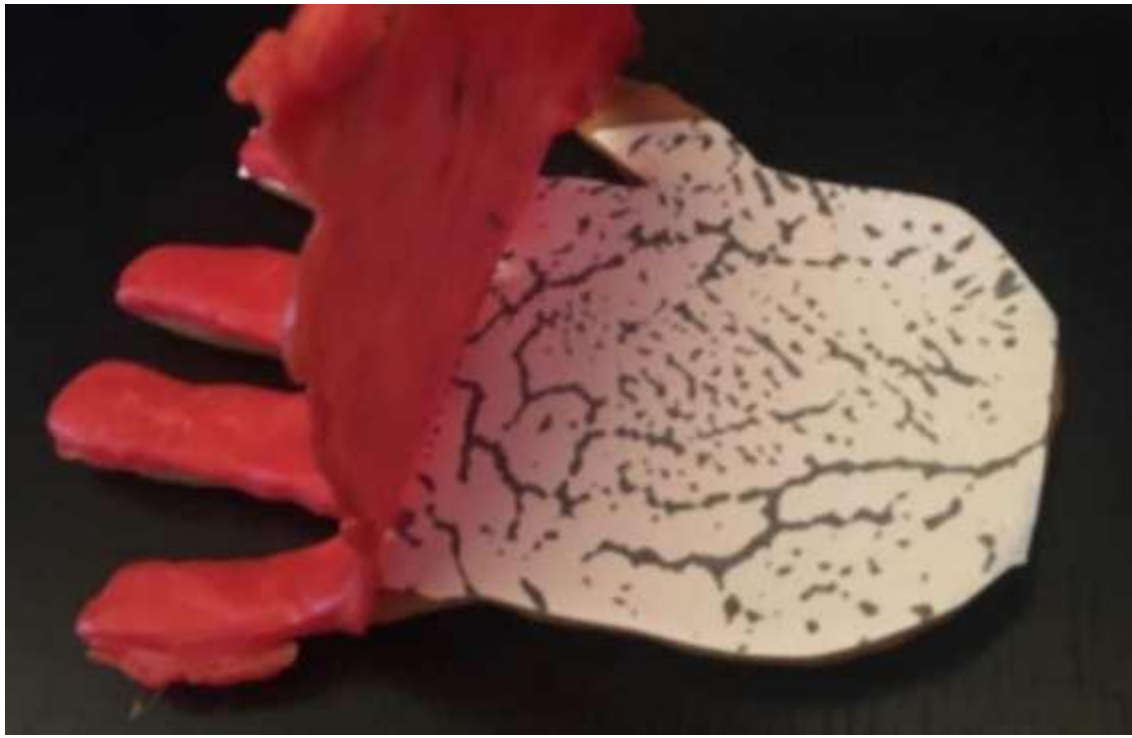
- The European Commission is looking for support to discover security flaws in some of the most popular free and open source software around.
- Rewards ranging from €25,000 to €90,000 ($28,600 to $103,000), for a total amount €851,000 ($973,000).
- Announced by Julia Reda, member of the European Pirate Party and co-founder of the Free and Open Source Software Audit (FOSSA) project, which was started in 2014 to help improve the overall security of the Internet, after severe vulnerabilities were discovered in key infrastructure components ? GUESS?

Filezilla	FLUX TL	KeePass	PHP Symfony	Apache Tomcat
Apache Kafka	VLC Media Player	7Zip	GNU C Library (glibc)	WSO2
Notepad++	PuTTY	Drupal	Digital Signature Services (DSS)	MidPoint

Hackers crack vein authentication security

Jan 1

- Hackers have constricted a fake hand out of wax and used this to show the weaknesses in vein authentication software.
- The software, which scans the vein patterns in hands and compares them to stored images, is not as robust as security experts thought.
- With the photograph, the hackers took the image using an SLR camera that had its infrared filter removed. By disabling the infrared filter, they were able to see the person's vein layout.



Your Exchange server can be pwned by an email (and other bugs need fixing)

Jan 8

- Micrsoft released 49 bug fixes, including patches for remote code execution flaws in DHCP (CVE-2019-0547) and an Exchange memory corruption flaw (CVE-2019-0586) that is particularly dangerous as it can be exploited simply by sending an email to a vulnerable server.
- A vulnerability (CVE-2019-0547) was discovered internally by Microsoft Windows Enterprise Security Team, that could allow an attacker to send a specially crafted DHCP response to a client in order to perform arbitrary code execution on the client.
- This Patch Tuesday included security updates that fix two vulnerabilities (CVE-2019-0550 & CVE-2019-0551) in Hyper-V that could allow malware on the guest to execute code on the host operating system.

$7,500 Steam Weakness Let Hackers Take Remote Control Of Gamers' PCs

Jan 8

- The bug lay in the Steam Chat feature, according to Shadwell. His hack exploited the way in which that application handled what's known as "rich chat content."
- Many modern chat applications include 'rich content,' such as including a YouTube player with messages. The attack used flaws in the Steam Chat client's protections around this content to access normally restricted functionality that Steam uses internally to open files on the user's computer
- The best way to exploit the bug was to post a link to a gamer, which when clicked would launch the attack code and hand control over the victim's PC to the hacker.

It only takes a Skype Call to Unlock an Android Handset

Jan 10

- Florian Kunushevci, the bug hunter who identified the vulnerability (CVE-2019-0622), claims that a person owning Android phone can receive a Skype call without even unlocking the phone apart from accessing other data.
- Video->

Aussie Govt Emergency Service hacked to send fake warning alerts

Jan 7

- The security breach occurred over the weekend. Registered members of EWN.com.au were sent messages by the hacker that the system is hacked and their personal information has been exposed.

Unprotected MongoDB leaks resumes of 202M Chinese job seekers

Jan 11

- Reportedly, an unprotected MongoDB has exposed personal and professional details of more than 202 million Chinese people.
- The data belonged to the last three years and the reason behind its exposure is that it was stored in an unsecure and unprotected MongoDB database.
- The exposed database contained **854GB of data.**
- Diachenko couldn't identify any specific service associated with the database but he did discover a 3-year old repository on GitHub for an app. The app contained almost "identical structural patterns" as were part of the exposed resumed. Apparently, the data is scraped from Chinese classified services like 58.com.

Chinese hackers pulled off the Italian con job, a Rs 130-crore heist

Jan 11

- A gang of Chinese fraudsters stole $18.6 million (Rs 130 crore) from the Indian arm of Italian company Tecnimont SpA by convincing local managers that the money was needed for an acquisition.
- The hackers sent emails to the head of Tecnimont Pvt Ltd, that looked deceptively similar to that of group CEO Pierroberto Folgiero.
- The hackers then arranged a series of conference calls to discuss a possible “secretive” and “highly confidential” acquisition in China. Several people played various roles during these calls, pretending to be the group CEO, a top Switzerland-based lawyer and other senior executives of the company.
- The hackers convinced the India head that the money couldn’t be transferred from Italy due to regulatory issues. He then transferred the amount in three tranches during one week in November. The money that was transferred — $5.6 million, $9.4 million and $3.6 million to Honkong Banks.
- The fraudsters tried for a fourth transfer, but by then the fraud had been discovered. It came to light when Tecnimont SpA chairman Franco Ghiringhelli visited India in December.

Personal data of German political elite dumped online

Jan 04

- The vast trove of data was released online and disseminated via Twitter over the span of four weeks – without anybody really noticing.
- The smorgasbord of leaked data includes the politicians' credit card details, banking and financial information, addresses, mobile phone numbers, photos of ID cards, personal chat histories, as well as their respective parties' emails, memos and letters

Jan 09

- The Guardian reports that Germany's federal police agency (BKA) has apprehended a 20-year-old student who has confessed to being behind the incident that affected around 1,000 people, some 950 of which are politicians.

</End>

That's All!

I will be sharing this presentation on my GitHub Account (and last month's presentation of CHFI)

https://tinyurl.com/NMMumbai

Thank you