ORACLE

Securing your Open Source Infrastructure

Ankur Pahwa

Pre Sales Consultant
Oracle Linux & Virtualization

November 20, 2019

Safe Harbor

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at http://www.oracle.com/investor. All information in this presentation is current as of September 2019 and Oracle undertakes no duty to update any statement in light of new information or future events.

Why Security is important?

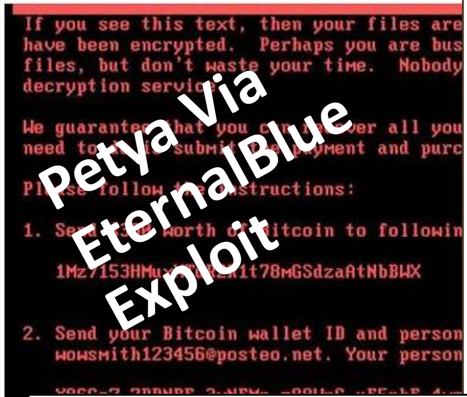
- Digitalization – Enterprise and Public
- Cloud Storage
- Digital Economy
- Smart City Setups
- IoT Devices

Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide

This isn't ransomware – it's merry chaos

28 Jun 2017 at 03:19

SHARE ▼



```
If you see this text, then your files are
have been encrypted.  Perhaps you are bus
files, but don't waste your time.  Nobody
decryption servic

We guarantee that you can recover all you
need to submit the payment and purc

Please follow the instructions:

1. Send $300 worth of Bitcoin to followin

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and person
   wowsmith123456@posteo.net. Your person
```

An

na

bu

South Korean hosting co. pays $1m ranso end eight-day outage

Talked scum down from $4.4m after they waltzed throug unpatched legacy mess

By Richard Chirgwin 20 Jun 2017 at 03:02

Erebus Linux Ransomware

over US$1 million to

stomer video files an

e data.

Stack Clash flaws blow local root holes in loads of top Linux programs

We knew about this in 2005. And 2010. And people are still building without -fstack-check

By Iain Thomson in San Francisco 20 Jun 2017 at 01:03

SHARE ▼

Stack Clash

Powerful programs run daily by users of Linux and other flavors of Unix are riddled with holes that can be exploited by logged-in miscreants to gain root privileges, researchers at Qualys have warned.

Essentially, it's possible to pull off a "Stack Clash" attack in various tools and applications to hijack the whole system, a situation that should have been prevented long ago.

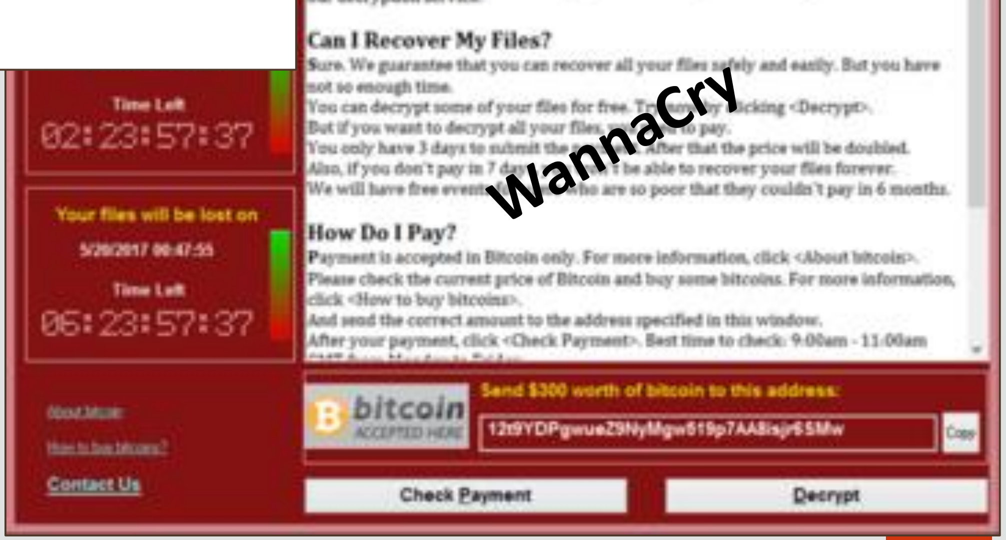
Linux Servers Hijacked to Mine Cryptocurrency via SambaCry Vulnerability

June 10, 2017 04:30 AM

An unknown threat actor is using a vulnerability in Samba installations to take over Linux machines and use them as pawns in a vast cryptocurrency mining operation.

According to public data, their actions started about five days after the Samba team announced they patched CVE-2017-7494, a vulnerability in all Samba versions released since 2010.

Because the vulnerability is exploitable via the SMB protocol, and because the issue came to light so close to the WannaCry ransomware outbreak, some researchers started referring to the bug as **SambaCry** or **EternalRed**.



Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

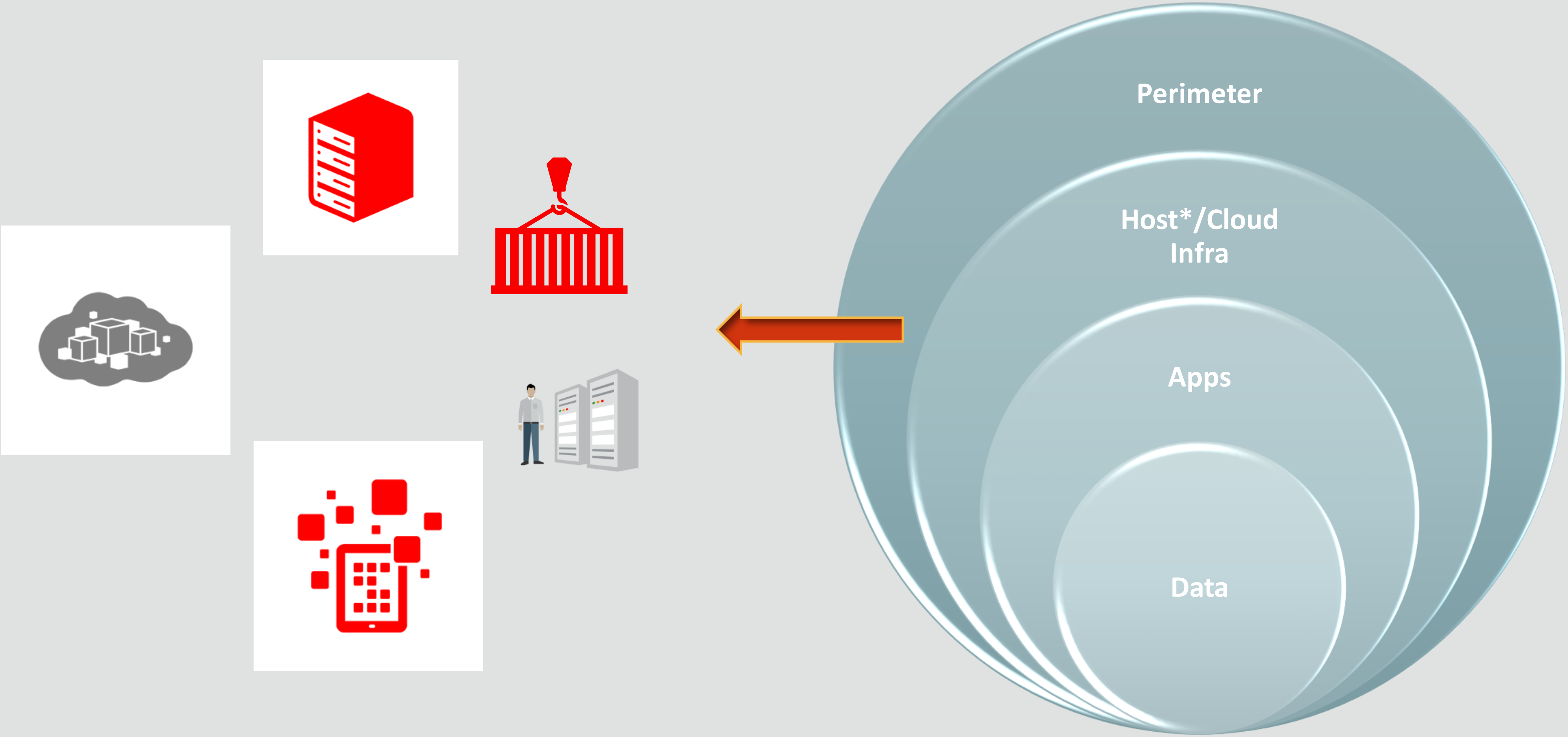
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Source : https://www.theregister.co.uk , https://www.bleepingcomputer.com

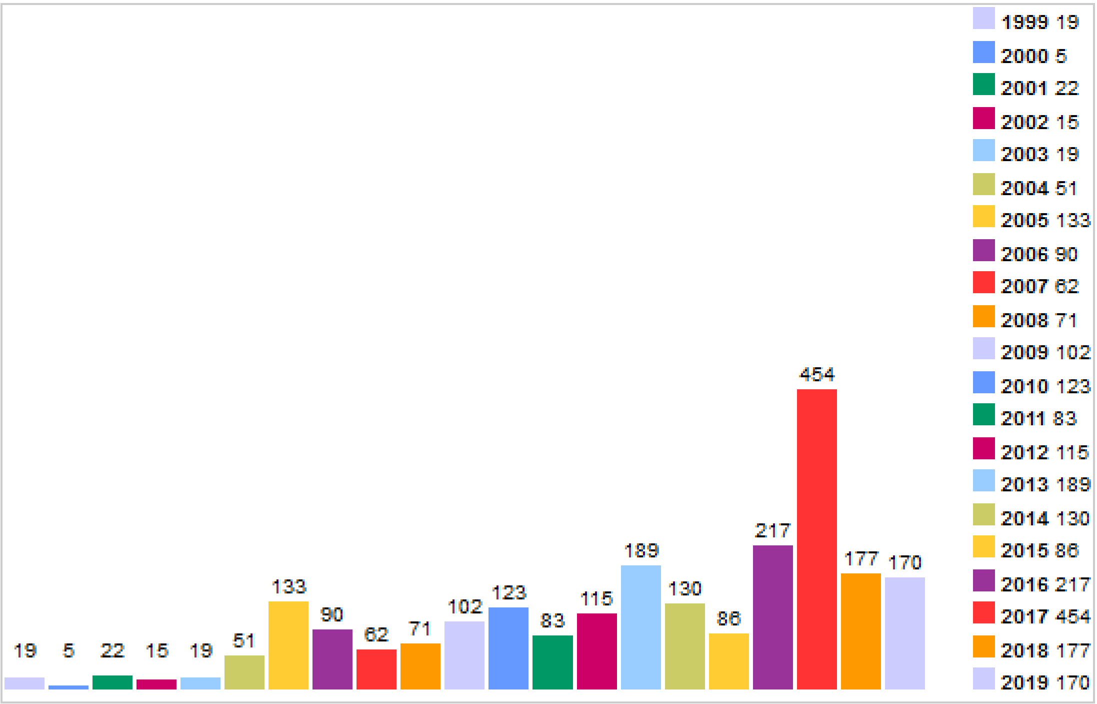
No “Silver Bullet” for Security

Think “Defense in Depth”, especially in today’s software-defined world

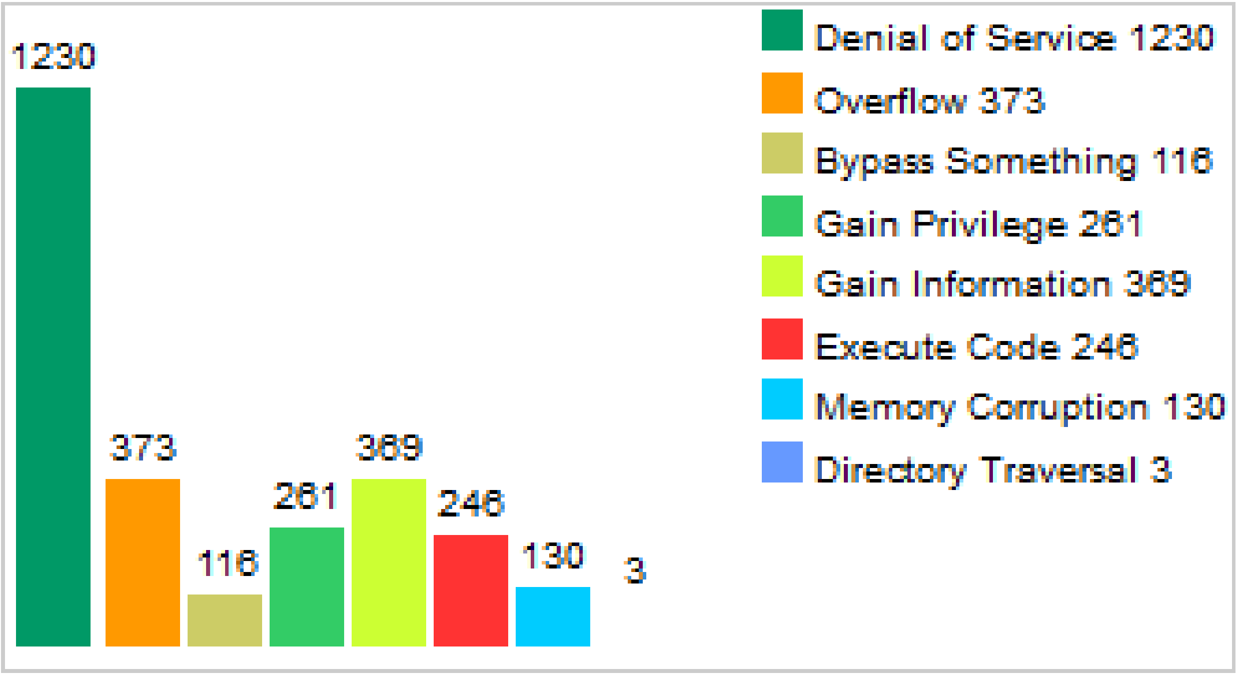


Do you also consider Operating System Security?

Vulnerabilities by Year



Vulnerabilities by Type



- CVE-2018-14634 Mutagen
- CVE -2016-5195 Dirty Cow
- Heartbleed - openSSL

Source: https://www.cvedetails.com/product/47/Linux-Linux-Kernel.html?vendor_id=33

Ksplice Live Patching Applies Security Patches While Running

- Rapidly patch zero-day vulnerabilities with no downtime
  - Kernels
  - Hypervisors (KVM, Xen, and QEMU)
  - Critical user space packages (glibc and openssl)
- Keep critical systems patched with no downtime
  - 100,000s of Oracle Cloud servers patched in hours
- Proven: 1 million+ patches delivered

Always Secure.

Known Exploit Detection

- As CVEs are patched, Ksplice adds ’tripwires’ to code that fire when erroneous conditions are triggered
- Helps report attempted exploitation of a known attack vector
  - Default is to log exploit attempt to syslog; email alerts can also be set
  - You can take specific action for specific tripwires (report/ignore)
- Helps system admins monitor systems for suspicious activity

Highly Secure.

Autonomous Linux Reduces Downtime

- Automatic OS maintenance

  Performs patching and updating while the system is running

  Patches are fully tested by Oracle to validate updates don’t break compatibility
- Eliminating human errors means 99.995% availability: total downtime less than 2.5 minutes per month
- Another reason why Oracle is …

Highly Reliable.

Stay Connected

Twitter.com/oraclelinux

Facebook.com/oraclelinux

Blogs.oracle.com/linux

YouTube.com/oraclelinuxchannel

Visit us at oracle.com/linux