The Coming Malware Storm

How to Defend BroadWorks Against Malware Like *WannaCry* and *NotPetya*

www.ecg.co

One Operating System Bug:
$53 Billion in Damage.
Outages lasting weeks.

On March 14, 2017, a patch was released to repair a bug in server operating systems. Network administrators around the world didn't know at the time, but they had exactly 60 days to install the patch. On May 12, the WannaCry ransomware attack was unleashed, attacking computers around the world that had not yet installed those patches. Then on June 27, a second, more destructive attack was launched: NotPetya.

The IT world reeled. Maersk global logistics shipping was slowed. Fedex suffered damage. Those logistics companies alone reported losses in excess of $600 million due to the attacks.

Healthcare was impacted, with Merck Vaccine production shut down in the US. Surgeries and lab work in the UK were cancelled. Nuance Communications outage slowed transcriptions and records for patients.

Recovery in some networks took months. In the months following the attack, Lloyds of London estimated the total worldwide cost of the attacks at $53 billion.

Impacts on Telecom & Core Infrastructure

Two telecom providers, Télefonica and Portugal Telecom, both reported infection. Computing staff at Télefonica asked end-users to shut down their computers and shut down corporate VPNs, according to news site *Bleeping Computer*. Security Affairs also reported problems at Vodafone.

Beyond telecom to other core infrastructure, the Spanish newspaper El Mundo reported that Iberdrola Electric Utility was also affected.

I cannot defend American espionage using incredibly powerful tools if we cannot keep them secret.

General Michael Hayden, September 21, 2017

Photo: Gettys

Et tu, Linux?

The two back-to-back attacks, NotPetya and WannaCry, exploited a Microsoft operating system vulnerability weaponized as "EternalBlue" by the American National Security Agency (NSA), and subsequently leaked. Congressman Ted Lieu (D) of California claims the NSA purposefully kept the vulnerability as a secret weapon, choosing not to report it to the operating system vendor for years. Former NSA and Central Intelligency Agency (CIA) chief, General Michael Hayden, expressed concern last month that the US Government shouldn't be hoarding exploits. "I cannot defend American espionage using incredibly powerful tools if we cannot keep them secret," Hayden said at a conference September 21, 2017.

While EternalBlue exploited a Microsoft vulnerability, most core Telecom infrastructure runs on Linux. **Evidence is growing that the NSA is hoarding, and leaking, vulnerabilities on Linux systems.** For example, the "Vault 7" leak from the CIA via the Shadow Brokers shows advanced attacks on Linux using iptables and SSH, according to Cybereason.

With Linux targeted by the CIA and NSA, voice system operators from BroadSoft BroadWorks, Metaswitch, Genband, OrecX Call Recording, and NetSapiens are in the crosshairs. In 2012, Microsoft was reportedly running Skype services on Linux.

When did you last Patch the OS?

In June 2017, Washington Post reported that North Korea was the suspected origin of WannaCry. Attacks launched on the Internet can spread to cause collateral damage in every network. The world had only 60 days between the release of an operating system patch, and the havoc of WannaCry. This leads responsible system operators to ask: What was disclosed 60 days ago that needs to be patched today?

Defending Core BroadWorks Infrastructure against Attack

BroadSoft BroadWorks is a leading platform for Unified Communications ("UC"), controlling, routing, and mixing audio, video, conference calls, instant messages, faxes, and voicemails among millions of users every day. The firm believes that by 2020, 41% of real-time communication services will use a hosted platform, like Broadworks or its competitors.

> *"After an installation, the first task to perform is to update Red Hat with the latest available updates."* BroadSoft

BroadWorks, along with practically all other Carrier-Grade UC platforms, is software built to run on Linux. Operators prepare Linux servers and virtual machines, installing BroadWorks software on top of that Linux platform.

Lesson #1: Be Prepared for Linux Operating System Updates

Updating modern operating systems requires patches to be readily available, a lab in which to test, and a working fault-tolerant platform.

Readily Available Patches. Most BroadWorks operators are running on Red Hat Enterprise Linux (RHEL). But too many of them fail to maintain the RHEL subscription required to receive the newest updates. Keep this RHEL access up to date for all the servers. This pays Red Hat for the valuable service of integrating security fixes into their software releases.

Even if you have RHEL access, many BroadWorks servers cannot connect directly to Red Hat to download the software due to firewall rules. It is possible to allow a BroadWorks server to connect outbound to Red Hat repositories without allowing it unfettered access to the global Internet. Alternately, you can build a local repository using Red Hat Satellite or SpaceWalk.

Lab. Every BroadWorks network has a lab. However, well-run networks have a separate production network, too. That is: either you can test in a separate and distinct lab environment, or you can subject your customers to the testing; but in either case, testing will occur. A proper lab mimics enough of your production network to allow you to test all of your features and services, including fault tolerance.

Redundancy & Fault Tolerance. One of the most important features for a voice and UC service provider is *reliability*. The key to reliability is fault tolerance: the capability to keep offering services even when a fault occurs in the network. Fault tolerance is usually implemented with *redundancy*: (a) the presence of multiple identical replicas, such as a primary and secondary Application Server (AS), (b) either of which can provide the services, (c) either of which is ready to take over at any moment, and (d) which can recover the redundancy automatically after the fault.

Every BroadWorks operator has a lab.
Well-run networks have a separate Production Network, too.

To keep systems up to date, you need the ability to shut down one server at a time, and perform its updates. Without redundancy, if you shut down a server, you lose all the services provided by that server.

Most production BroadWorks networks have redundant Application Servers. Some, however, lack suitable redundant Profile Servers, so that when the OS on this key server is updated, provisioning of new users and services, Call Center Reporting, and SIP phone configuration is interrupted.

The lab benefits from redundancy as well, to allow thorough testing of the patches, and the interactions of servers. A BroadWorks lab without redundancy means that the production platform is used for all testing of the redundancy functions in BroadWorks.

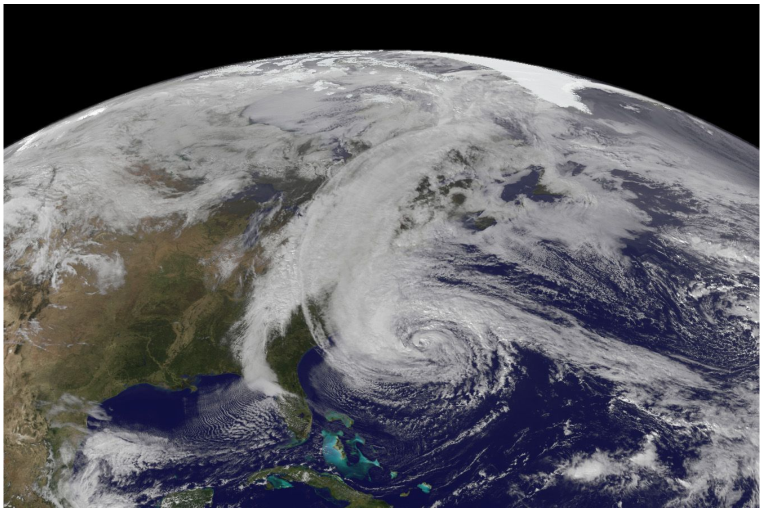


Photo: NASA GOES.

Lloyds of London estimate the Malware damage at $53 billion, 71% of Hurricane Sandy's cost.

Lesson #2: Keep Systems Patched and Up-to-Date

The Institute of Electrical and Electronics Engineers (IEEE) urges that with WannaCry and Petya, those system that did not patch quickly enough -- in the 60 day window -- suffered from the attack. ComputerWeekly reminds us that the **permanent damage** of NotPetya could have been prevented for all those victims by maintaining the operating system, installing the available patches.

Red Hat is a leading vendor and maintainer of the Linux OS. Gartner reports that two out of every three Linux machines are running Red Hat Linux. 75% of Red Hat's revenue comes from Red Hat Enterprise Linux subscriptions, which provide security updates to customers. Red Hat issues bug fixes and security updates nearly every day of the year. (Many of these updates are distributed downstream to the Open Source community via CentOS.)

Starting Out Right

When you install the Linux OS for a new BroadWorks server, BroadSoft requires that the system be updated to the latest patch level According to the official specifications frmo BroadSoft in the Software Management Guide, "After an installation, the first task to perform is to update Red Hat with the latest available updates," While you can sometimes accomplish the installation from non-updated DVD sources, this approach leaves the server unpatched against vulnerabilities, and unprepared for new malware.

Maintain Patches With Network Stability, too

First: OS Patch Lab Testing. Operating system patching must be tested with the BroadWorks application. Operators use Linux only because it enables them to run BroadWorks. The application must be thoroughly tested with each patch.

Operating system patches should be applied in a lab environment, then *all supported* features and services should be tested on the updated platforms. This means *everything that a customer may use* should be tested. For voice and UC service providers, these tests should exercise all the major features of the platform:

- Ordinary voice calling and caller ID
- Call hold and retrieve, hunt groups, auto attendant, call center / ACD
- PSTN calling inbound and outbound, with DTMF transfer
- Conference calling, both meet-me and N-Way conferencing
- Deposit and retrieval of voicemail, by BroadWorks Voice Portal (Telephone User Interface, TUI) and email
- Fax delivery
- Receptionist Console

- Instant messaging, presence, desktop sharing, and video calling

Never neglect to test these key functions, behind the veil of normal customer service:

- SIP phone configuration file generation and retrieval, TLS client authentication
- Failover and fault tolerance between Application Servers (AS), Profile Servers (PS), Database Servers (DBS)
- Provisioning new users, and SIP access devices, soft clients

> ***The Vault 7 leak shows the CIA is working on new exploits for Linux servers, and that the exploits will be leaked to hackers.***

Testing must confirm that all functions work properly with the new operating system patches. Fortunately, BroadWorks is built to integrate properly with Red Hat Linux, so the changes to the OS affect the application only rarely.

Second: Phased Rollout in Maintenance Window. After lab testing demonstrates that the operating system updates work properly with the BroadWorks application *in your specific networks*, install the OS updates in the production network in a maintenance window, i.e., at the part of the day where your usage is minimized. There are two common methods of options on the order in which you run OS updates:

1. **Primary servers first:** Shut down your BroadWorks "primary"[1] servers, e.g., AS1 (Application Server), PS1 (Profile Server), NWS1 (Network Server), MS1 (Media Server), XSP1 (Xtended Services Platform - Web Server), UMS1 (Unified Messaging Server), USS1 (Unified

[1] *In this section, the term "Primary Servers" and "Secondary Servers," is used, though in BroadWorks only certain servers have primacy. For example, all Network Servers are equal. XSPs are only primary for limited purposes, like Web Branding mastership. But Application Servers do have a preference: for consistency of call state, the system prefers to have all calls active in a cluster on the primary member of the cluster. I use the term "Primary" to refer to the "#1" servers, and secondary to refer to the "#2" servers. For a network with larger clusters, e.g., three Network Servers, then the model must be extended.*

Communication Screen Share Server.), etc. causing a failover to your secondary servers. Then update the OS on all the offline servers. Restore them, and bring the traffic back to the primary servers. This has the advantage that if a problem is detected after the primary servers have been updated, you can shut down a primary server, and then fail-over to the older servers, which haven't been patched yet.

2. **Secondary servers first:** While the primary servers are still taking providing service, patch the "secondary" servers, such as AS2, PS2, etc. Then when the OS patches are completed, shut down the primary servers to force failover to the secondary servers. This allows you to test traffic on the secondary servers, and if a problem is discovered, merely restart the primary servers.

Lesson 3: Once Infected, Replace the OS

Once a server has been exploited, you can no longer trust the operating system. It has to be replaced. As Fortune Magazine reported in June 2017, the NotPetya malware modified the Master Boot Record, part of the OS.

It can be tempting to think of Malware as a simple infection: once "cured" you never need to worry again. But Malware can hide inside the operating system; as Cybereason reported, the Vault 7 release includes evidence of CIA or NSA malware that can hide inside Linux iptables or SSH. So, once you are aware a server has been compromised, the server OS has to be replaced.

Responsible OS Replacement in BroadWorks Linux Environment

When you discover a server has been compromised in the past, you need to replace its operating system, even if it appears the malware is inactive.

1. Ensure you have a Truly-Redundant alternate server. Test your failover to be sure the other server is functional, and all the failover mechanisms (such as SBC configurations, PSTN gateway setup, and timeouts) are working properly.
2. Remove the peer from redundancy on the alternate server. (E.g., if AS1 is compromised, make AS2 the primary server in the cluster, and delete AS1 with *peerctl*.)
3. If the compromised server is a bare-metal (non-virtualized) server, then physically format and reinstall the Linux operating system. If the compromised server is a virtual machine, then shut down and delete the virtual machine.
4. Patch and update the OS, then install BroadWorks. Add it as a peer with the alternate server.

For the current procedures for removing a peer and adding a peer, see the current BroadWorks Maintenance Guide.

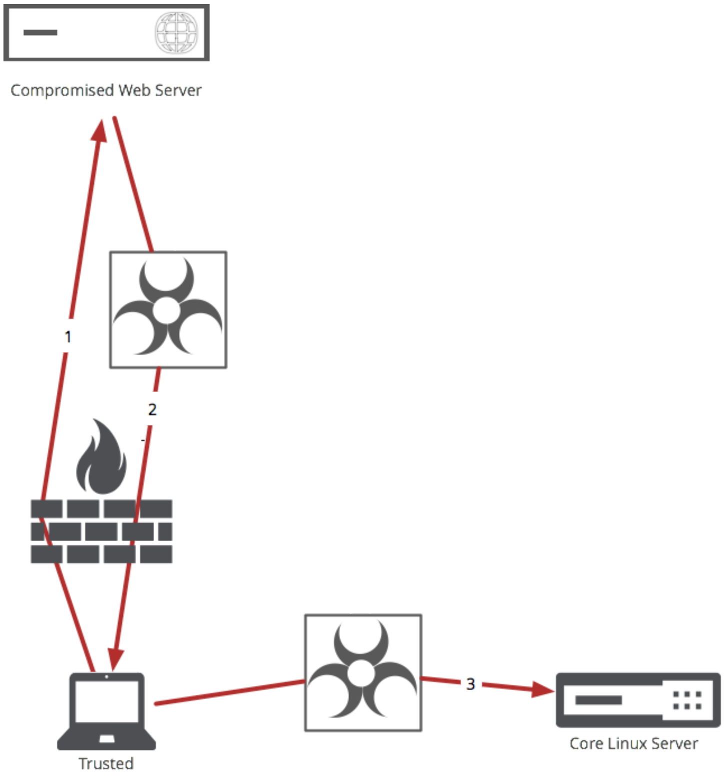
Without a redundant lab, you're not prepared to test Operating System Updates.

Lesson 4: Firewalls Help, Sometimes

WannaCry and NotPetya spread across the local area network (LAN), according to Palo Alto Networks. But the primary delivery tool was software updates when client software downloaded an exploited application. Neither path is protected by firewalls: software updates just look like ordinary web traffic, and firewalls typically don't limit traffic within a LAN subnet.

As PublicTechnology reports, firewalls can help prevent the spread of malware from client PCs, like Windows computers, to your core Linux servers. We should expect malware that is distributed from desktop PCs to attack the core network.

Firewalls should minimize access between your PCs, Macs, Android and iPhone clients to the core network. Too many voice and UC operators have insufficient firewall restrictions that fail to defend their core servers against attacks launched from staff PCs.



Trusted Devices inside your firewall can inadvertently be compromised. Then, malware can attack your core Linux systems. Firewalls should protect your core network against trusted users as well as the Internet.

Lesson 5: Linux Malware Is Here, with More Coming

History has shown us that every platform has malware, and Linux is no exception. Sophos documents examples of Linux malware. Canonical, makers of Ubuntu Linux, document a long list of Linux exploits. And Hacker News documented in June 2017 how the American Central Intelligency Agency (CIA) is developing new exploits for Linux.

Lloyds' of London's estimated the global economy paid $53 billion due to WannaCry and NotPetya. This approaches the scale of Hurricane Sandy, which struck the United States in 2012, and cost $75 billion.

BroadWorks operators take steps to prepare for natural disasters, and must defend against malware attacks that will be launched against their core servers' operating systems. By maintaining the OS on a routine, repeated, continuous basis, voice and UC operators can provide ongoing protection against the inevitability of destructive Linux malware.

ECG offers voice and UC technical consulting for national governments, higher education, telecom software vendors, and the healthcare industry. ECG offers Alpaca, the only management tool for large-scale BroadWorks installations, along with patching, troubleshooting, and 24x7 monitoring of critical network services.

info@ecg.co
www.ecg.co

Research & Content: ECG Technical Staff

Contact: Jan Walker, ECG, +1-229-316-0019