21 For 21
21 Things to Know/Try for a Better 2021

January 20, 2021

By Aaron Grothe
NEbraskaCERT

Introduction

21 for 21?

I did a 12 for 12 talk in 2012 and have just kept going from there. Used to say I was in a rut now describe it as a groove.

Links are at the end of the talk
Slides will be posted at the NEbraskaCERT website
http://www.nebraskacert.org/csf

Introduction (Continued)

If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.

OpenSMTPD Bug Analysis

The Register did a very nice little write up on a bug in the OpenBSD project's OpenSMTPD program.

Qualys found the initial issue and disclosed CVE-2020-7247

Bug is an issue of insufficient input validation. Email addresses are not handled correctly and commands can be included in the email.

Bug can be exploited through the use of netcat

OpenSMTPD Bug Analysis.

The size of the fix is less than 20 lines :-(

Is small, easy enough to provide a really good example of a bug

$5/month License Plate Reader.

Engadget article talks about a product called Watchman from OpenALPR that can be used to do license plate analysis.

The home owner version can recognize a license plate and send alerts to the user based upon whitelisting and blacklisting the license plates.

They also offer the same license plate recognition technology to business from $50/month.

Will leave the possibilities of abuse for this to the reader :-)

Firewall Features for Pros.

Many people still think of firewalls in terms of being simply routers. A lot of them can do more.

This Network World article lays out 5 features that a lot of higher end firewalls offer

Network segmentation
Policy optimization
Credential-theft prevention
DNS Security
Dynamic User Groups

Huawei Cyber Security Evaluation

Huawei is an interesting company.

- They are a major player in the 5g rollouts in many countries
- They are a Chinese company
- The US has put severe restrictions on them in the U.S. and for many of our allies
- As part of an attempt to continue to be able to sell into countries such as the U.K. they have created an evaluation center oversight board
- They've been doing the reports for the last 6 years
- The 2020 version of the report has been published
- As more infrastructure continues to come from other countries the Huawei/GQHQ type of situations are going to happen.

Huawei Cyber Security Evaluation.

Googling for "HUAWEI cyber security evaluation oversight board" will turn up the reports for the last 6 years.

Line from the 2019 report was interesting

> "HCSEC has continued to find serious vulnerabilities in the Huawei products examined. Several hundred vulnerabilities and issues were reported to UK operators to inform their risk management and remediation in 2018. Some vulnerabilities identified in previous versions of products continue to exist."

I Got Phished.

I Got Phished accepts data from "trusted IT-security researchers" to let people know about email addresses that have been victims of phishing attacks. How the researchers get the data is not disclosed.

You have to sign up as a domain admin abuse@email.com can't do as individual user

Only works on RFC 2142 supported email addresses (abuse, postmaster, noc, security) at the domain level.

Nice concept, and some of the statistics are interesting. Not sure how widely used it is.

Free Trial $72,000 bill

Register has an article about a startup by the name of Milkie Way and their founder who was an ex-google employee running up a bill of 72k overnight

Why this shouldn't have happened

Test was setup with $7.00 billing budget and a free database plan
Founder was an ex-Google employee
Credit card for account had spending limit of $100.00

Free Trial $72,000 bill.

How it happened

Was doing webscraping and didn't take into account that pages could link to each other
Dashboards took more than 24 hours to update so no notification - was million times ahead of what was shown

Was able to get them to forgive the bill as a "one-time gesture". Ex-google employee not sure it'd work for us

Cloud is still complex and have to be cautious about options selected

Massive Tech Grab for a WhatsApp User

U.S. Government attempting to work around limited information available via WhatsApp users

WhatsApp user is a suspected Drug dealer

Put in request to WhatsApp/Google and many other companies as part of one order.

Usually the U.S. Government has to put a request in which each telecom/tech provider.

Massive Tech Grab for a WhatsApp User.

Part of the request

- Identity of WhatsApp accounts created with same IP address
- Recovery email(s)
- Identity of all accounts linked to the account by cookies
- IP addresses of any websites or other servers to which the cellphone or devices connected
- Post-cut through dialed digits - numbers hit by user once a call is started

Pretty broad, will have to see how these evolve over time.

Ransomware using Driver to kill AV

Sophos does a really nice job describing how the RobbinHood malware is able to use vulnerable yet signed/legitimate kernel driver to compromise a machine

1. Ransomware gets toehold on network
2. Install the legitimate gigabyte kernel driver
3. Exploit vulnerability in driver to gain kernel access
4. Use kernel access to disable OS driver signature enforcement
5. Install malicious kernel driver rbnl.sys
6. Rbnl.sys disables security measures
7. Encrypt victim's files

Ransomware using Driver to kill AV.

This is impressive as it using a valid driver to get access to the system.

Verisign has pulled the signature validation for the gigabyte driver, but keep in mind the number of hardware manufacturers that are out of business or not actively patching their drivers and this can continue.

Is there a GPO (Group Policy) that can prevent the potential issues with drivers being automatically installed.

MacOS Gatekeeper

During the rollout of the Latest Version of Mac OS (Big Sur) some people were having issues launching applications.

The suspected culprit of this is an application from Apple called Gatekeeper that uses protocol named OCSP (Online Certificate Status Protocol)

OCSP sends HTML get-requests that aren't encrypted. Use the Apple-issued developer certificate. Included other information such as IP address and so on. Apple is revising this.

MacOS Gatekeeper.

Gatekeeper intentionally bypasses VPNs. So the basic information that was being provided is as follows

IP address
Apple Developer ID

Given this you can get a good idea if a user is running a "frowned upon app" such as whatsapp, tor, etc.

Turning off OCSP is pretty difficult, goes to the issue of whether or not you own your computer.

Leaking Data by Switching Ethernet Speed.

An example of switching the ethernet speed of machines to create a side-channel for data exfiltration.

Was pretty successful with a Raspberry PI 4, less so with a couple of Dell laptops.

Able to send data out at the rate of 1 bit every 2-5 seconds. And you thought 33.6k was slow

Raspberry PI project is called etherify

Interesting research into beating air gaps via various means.

Exploiting use-after free in Chrome.

Excellent write up of taking exploiting a user-after-free bug in an earlier version of Google Chrome.

Uses javascript to manipulate the underlying engine.

If you're interested in how to work on a hack against Google Chrome. Highly recommend this.

Capcom Write Up of Unauthorized Access

Capcom was the victim of ransomware

Apparently 1tb of data was stolen
Attackers demanded $11 million in bitcoin for a decryptor
Promised to delete stolen data after payment

What has been impressive is how CapCom has responded they've released a pretty detailed accounting of what was stolen.

Capcom Write Up of Unauthorized Access

High level overview of disclosure

Information verified to be compromised
- Personal information of employees
- Sales reports
- Financial information

Potentially compromised
- Personal information customers, business partners, etc - 35k items
- HR information - 14k people
- Confidential corp information
  - Sales data, business partner information, dev documents, etc.

Capcom Write Up of Unauthorized Access.

Detection and Action taken
- Timeline for realizing compromise
- Discovery of notice from Ragnar Locker
- Issue of initial press release

Measures going forward
- Coordinating with law enforcement
- Consulting with external security experts

Actually a pretty short document that should be reviewed by anybody affected by Ransomware or concerned about it.

Finding Vulns in Code: Bad Words.

Interesting blog article by Will Butler about grepping for bad words to look for in security code.

Some to look for

validate|verify - places to look for input validation
Todo|fixme|xxx - danger words
Eval|exec|run - exec(code) dangerous in python should evaluate
Password|passwd - point to potential password issues

A nice high level article to help you figure out where to prioritize your code analysis time

FBI report on Drovorun Linux Malware

Report from the NSA and FBI talking about the Drovorun Linux malware.

Malware written by GRU - Russian intelligence

Consists of a kernel module, file transfer and port forwarding tool and connects to a command and control server.

Write Up is interesting, kernel module works to hide the malware, but network monitoring such as snort should be able to detect it.

SSH Honeypots.

Person setup a simple SSH Honeypot on multiple services (Digital Ocean, Google Cloud and NameCheap).

Provides breakdown of top 10 passwords/usersnames, etc. Most common countries, etc.

Usernames: “root”, “admin”, “user”, “test”, “oracle”
Password: blank, “123456”, “admin”, “123”, “1234”

Nothing really surprising in the results, but not a bad source of a bit of information. Pretty much lines up with my anecdotal info from the NEbraskaCERT server

CrowdSec Crowd-Src Fail2ban like system

CrowdSec is a distributed system based on the concepts of Fail2ban.

You install a client it processes (log files, streams, tails, messages, …) and normalize and enriches them.

Will use a bouncer for remediation, block, 403, captcha (soon), 2FA, etc.

CrowdSec Crowd-Src Fail2ban like system.

Interested to see if anybody will attempt to DoS the system with bad data.

Designed to be lightweight, supposedly ideal for docker and other container based systems.

Interesting project, will have to see how it moves forward

Current State of Exploit Development.

CrowdStrike put together a two part series on the current state of the art of OS hardening methods and ways to circumvent them.

Couple of the mentioned techniques

No-eXecute (NX), DEP - marking data pages not executable
Address Space Layout Randomization (ASLR)
Page Table Randomization
ACG - Arbitrary Code Guard

Most of them are Windows based, some have Linux counterparts

US Gov't buys Cell Phone Location Data.

U.S. Government bought access to commercial database that tracks the movement of millions of cellphones in U.S. To be used by Immigrations and customs.

Information is collected from phone apps by a company named Venntel. Venntel collects it from a variety of companies via apps on mobile phones: gaming, weather, and other apps are being used to collect this information.

There are strict laws limiting what data the government can collect on you, but there are no real rules preventing the Government from buying commercially available data.

HackadayU: Ghidra Class on Youtube.

Ghidra is a reverse engineering tool written by the NSA. Ghidra has been released as Open Source software and is available in github.

HackadayU has released a four hour introductory course to reverse engineering using Ghidra. Really good course goes from introduction to patch diffing and analysis, to how to use extensions.

Their youtube channel also has some other really good stuff on it as well. Highly recommend taking a look at their content.

FireEye Hacked.

FireEye was hacked apparently by a Nation State. Their "Red Team" tools have been stolen.

This is a unique situation in several ways

- FireEye is releasing information about their tools so defeneses can be written. This is the crown jewels for a lot of companies
- Little information about the attack has been released. FireEye will hopefully be very open about the attack
- Probably not as bad as NSA tools release as a lot of FireEye's tools are based upon tools they encounter during their investigations

DoD to Require CyberSecurity Certification from Defense Certs.

United States Department of Defense will require defense contractors to meet a basic level of CyberSecurity standards for answering proposals by 2026.

Cybersecurity Maturity Model Certification (CMMC) framework version 1.0 was released January 2020

Five Levels: from “1 basic cyber hygiene” to “5 optimizing”

Freenom.

Freenom is a free domain name registar. Allows you to sign up for domain names in .tk/.ml/.ga/.cf/.gq

Not trusted by all browsers/utilities.

Can be very handy for demos/practice phishing and pointing to internal resources. E.g. you can put a request in for 192.168.0.xxx and have it resolve on your internal network.

Links

Tip - OpenSMTD Bug Analysis

https://www.theregister.com/2020/01/30/openbsd_mail_bug/
https://nvd.nist.gov/vuln/detail/CVE-2020-7247

Links

Tip - License Plate Reader

https://www.engadget.com/2020-01-30-watchman-openalpr-homeowners-launch.html

https://www.cnet.com/news/this-company-could-turn-every-homes-camera-into-a-license-plate-reader/?UniqueID=90814D16-4360-11EA-933A-FDA0FCA12A29&ServiceType=twitter&TheTime=2020-01-30T13:01:00&PostType=link&ftag=COS-05-10aaa0b

Links

Tip - Firewall Features for Pros

https://www.networkworld.com/article/3519854/4-firewall-features-it-pros-should-know-about-but-probably-dont.html

Links

Tip - Huawei/Cyber Security Evaluation

https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2020

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923309/Huawei_Cyber_Security_Evaluation_Centre_HCSEC_Oversight_Board-_annual_report_2020.pdf

Links

Tip - I Got Phished

https://igotphished.abuse.ch/
https://tools.ietf.org/html/rfc2142

Tip - Free Trial, $72,000 bill

https://www.theregister.com/2020/12/10/google_cloud_over_run/

Links

Tip - Massive Tech Grab for a WhatsApp User

https://www.forbes.com/sites/thomasbrewster/2020/01/29/a-problematic-government-order-forces-tech-giants-to-help-hunt-a-whatsapp-drug-dealer/?ss=cybersecurity&sh=31e287a32516

Links

Tip - Ransomware using Driver to kill AV

https://www.zdnet.com/article/ransomware-installs-gigabyte-driver-to-kill-antivirus-products/

https://news.sophos.com/en-us/2020/02/06/living-off-another-land-ransomware-borrows-vulnerable-driver-to-remove-security-software/

Links

Tip - MacOS Gatekeeper

https://www.forbes.com/sites/johnkoetsier/2020/12/05/surprisingly-a-massive-and-ongoing-apple-privacy-breach-is-thanks-to-apples-security-focus/?sh=57f4338151f2

https://arstechnica.com/gadgets/2020/11/mac-certificate-check-stokes-fears-apple-logs-every-app-you-run/

Links

Tip - Leaking Data by Switching Ethernet Speed

https://hackaday.com/2020/11/30/leaking-data-slowly-by-switching-ethernet-speeds/

Links

Tip - Exploiting use-after free in Chrome

https://securitylab.github.com/research/CVE-2020-6449-exploit-chrome-uaf

https://github.com/github/securitylab/tree/main/SecurityExploits/Chrome/blink/CVE-2020-6449

Links

Tip - Capcom Writeup of Unauthorized Access

Initial information about access

https://www.capcom.co.jp/ir/english/news/html/e201104.html

Update on unauthorized access

https://www.capcom.co.jp/ir/english/news/html/e201116.html

Links

Tip - FBI report on Drovorun Linux Malware

https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

Tip - SSH HoneyPots

https://systemoverlord.com/2020/09/04/lessons-learned-from-ssh-credential-honeypots.html

Links

Tip - CrowdSec Crowd-Sourced Fail2ban like system

https://github.com/crowdsecurity/crowdsec/

https://doc.crowdsec.net/

Links

Tip - Current State of Exploit Development

Part 1 - https://www.crowdstrike.com/blog/state-of-exploit-development-part-1/

Part 2 - https://www.crowdstrike.com/blog/state-of-exploit-development-part-2/

Links

Tip - US Gov't buys Cell Phone Location Data

https://yro.slashdot.org/story/20/02/10/0044209/us-govt-buys-location-data-for-millions-of-cellphones

Links

Tip - HackadayU: Ghidra Class on Youtube

https://www.youtube.com/watch?v=d4Pgi5XML8E&list=PL_tws4AXg7auglkFo6ZRoWGXnWL0FHAEi

https://github.com/NationalSecurityAgency/ghidra

Also nice talk from Kernelcon as well

https://www.youtube.com/watch?v=KL1jE9dxas0

Links

Tip - FireEye Hacked

https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html

Tip - FreeNom

https://www.freenom.com

Links

Tip - DoD to Require CyberSecurity Certification from Defense Contractors

https://www.bleepingcomputer.com/news/security/dod-to-require-cybersecurity-certification-from-defense-contractors/

https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html