

Towards Integrated Cyber Preparedness for Alaskans



Alternate title



Disclaimers

My interpretation of community consensus

Test and weigh risk all tips *for your environment*

I am not a lawyer and this is not legal advice

Your organization or jurisdiction may be different

I do not speak for any employer, past or present



ArcticCon - Oct 4, 2018

Credit:
thoughtleadersllc.com

About me

ISP scars

Independent security researcher

\$DAYJOB in infosec in the telecom sector

Password auditor and enthusiast

Hills I'll die on: spaces, vim, Oxford comma, adblocking

About you

- IT / implementors
- SOC / responders
- Compliance / audit
- Engineers / architects
- Decision makers

Overview

The Alaskan Paradox

The public Alaskan attack surface
(and your own)

Being a good Alaskan cyber neighbor

Coordinated security in the Last Frontier?

The Alaskan Paradox

- We are logically small, yet physically large
 - ... small enough to survey our Internet space
 - ... large enough to make remote maintenance risky
- We have critical infrastructure
 - ... enough to be a target
 - ... sometimes not enough to fully fund security
- Our population is small ...
 - ... everyone knows everyone else
 - ... but everyone knows everyone else

The Alaskan Attack Surface (and yours)

Alaskan attack surface: IPs - limitations

- Virtual hosting & cloud – harder to filter on “Alaska”
- On mobile data, **Mobile IP** is controlled by provider
- If firewalls block scans, obviously no results
- Some services (SSL/TLS) are hostname-based

Alaskan attack surface: BGP sources

3724	State of Alaska		32204	KPU
7782	ACS		32643	Resource Data
8047	GCI		32786	Ravn
10538	TelAlaska		33751	Bartlett Regional Hospital
11090	MTA		36056	ANMC
14608	Alaska Fiberstar (ACS)		40226	Alaska USA
16512	GCI		46932	Anchorage School District
18443	Alyeska Pipeline		53942	Cordova Telephone
21528	AlasConnect		54925	FNSB School District
22079	Alaska Power & Telephone		54970	Northern Air Cargo
27575	Providence		393276	Chugach Electric
31896	Futaris		395401	Whitestone

Not exhaustive; not yet included: post-2017; some BGP downstreams of AT&T or Verizon

<https://www.techsolvency.com/alaskan-networks/>

Alaskan attack surface: IPs - CIDR blocks

12.12.105.0/24	72.5.96.0/23	162.218.128.0/21	199.33.240.0/24	204.238.26.0/24
23.135.128.0/24	72.5.104.0/22	162.219.64.0/22	199.58.52.0/24	205.159.28.0/24
23.235.96.0/20	72.5.111.0/24	192.75.0.0/24	199.58.55.0/24	205.159.91.0/24
24.237.0.0/16	72.35.96.0/19	192.83.242.0/24	199.59.216.0/22	205.166.26.0/24
31.207.56.0/22	72.42.128.0/18	192.147.40.0/24	199.116.8.0/21	206.174.0.0/17
63.140.64.0/18	74.114.80.0/21	192.161.132.0/22	199.165.64.0/18	206.223.192.0/19
64.4.224.0/20	74.123.240.0/22	192.189.215.0/24	199.189.128.0/22	208.69.196.0/23
64.74.176.0/23	74.124.64.0/18	192.189.216.0/22	199.192.192.0/22	208.69.198.0/24
64.186.96.0/19	75.95.144.0/20	192.189.220.0/24	199.200.6.0/23	208.82.68.0/22
65.74.0.0/17	104.171.96.0/20	192.206.58.0/24	199.249.161.0/24	209.112.128.0/18
66.58.128.0/17	104.254.224.0/21	192.234.153.0/24	204.17.139.0/24	209.112.192.0/19
66.151.168.0/22	107.152.112.0/20	192.245.44.0/24	204.17.140.0/24	209.124.128.0/19
66.223.128.0/17	137.229.0.0/16	198.17.216.0/24	204.17.169.0/24	209.161.160.0/19
66.230.80.0/20	138.32.8.0/21	198.22.174.0/24	204.29.174.0/24	209.165.128.0/18
66.230.96.0/19	139.60.224.0/23	198.51.13.0/24	204.62.233.0/24	209.193.0.0/18
67.58.0.0/19	146.63.0.0/16	198.99.16.0/21	204.80.136.0/24	216.67.0.0/17
67.59.96.0/20	151.169.16.0/20	198.99.24.0/23	204.89.222.0/24	216.115.112.0/20
69.25.217.0/24	151.169.112.0/24	198.160.252.0/24	204.90.103.0/24	216.137.192.0/18
69.161.0.0/19	158.145.0.0/16	198.163.32.0/21	204.107.95.0/24	216.152.176.0/20
69.162.192.0/19	161.129.28.0/24	198.183.169.0/24	204.126.118.0/23	216.252.161.0/24
69.178.0.0/17	162.211.56.0/21	198.185.228.0/24	204.238.24.0/23	

<https://www.techsolvency.com/alaskan-networks/>

Alaskan attack surface: IPs - TCP ports

Overall public IP space

- 759,040 IPs in “known” Alaskan space
- **~80,000** show at least one port open/closed/filtered
(based on the top 24 Nmap “discovery” ports)
- **21,767** of these have at least one port **open**

Alaskan attack surface: top TCP ports

Port	Service	Count
80	HTTP	13639
443	HTTPS	9015
22	SSH	4766
21	FTP	2704
23	telnet	2285
123	NTP	1763
25	SMTP	1168
445	SMB	1105
139	NetBIOS	1036
3389	RDP	920
515	print	490

Note: since many IPs are dynamic,
these numbers ebb and flow over time

Port	Service	Count
5900	VNC	484
135	MS epmap	463
3306	MySQL	212
500	ISAKMP	208
9100	print	203
199	SNMP multiplex	189
1433	MSSQL	163
5800	VNC	152
37	time	111
137	NetBIOS	94
5060	SIP	53

Alaskan attack surface: remote access

Risks

- Exposes credentials of the underlying authentication system
- No account lockout = vulnerable to password spraying
- No logging & alerting = attackers guess passwords forever
- Successful guesses *can then be leveraged elsewhere*

Alaskan attack surface: remote access

Mitigations

- Just. Turn. It. Off.
- Segment/geofence/ACL
- Throttling / lockout / CAPTCHA
- Logging on success and failure
- MFA, reverse proxy
- Strong passwords

Alaskan attack surface: RDP



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



Sep 27, 2018

Alert Number
I-092718-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

CYBER ACTORS INCREASINGLY EXPLOIT THE REMOTE DESKTOP PROTOCOL TO CONDUCT MALICIOUS ACTIVITY

BACKGROUND

Remote administration tools, such as Remote Desktop Protocol (RDP), as an attack vector has been on the rise since mid-late 2016 with the rise of dark markets selling RDP Access. Malicious cyber actors have developed methods of identifying and exploiting vulnerable RDP sessions over the Internet to compromise identities, steal login credentials, and ransom other sensitive information. The Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) recommend businesses and private citizens review and understand what remote accesses their networks allow and take steps to reduce the likelihood of compromise, which may include disabling RDP if it is not needed.

DEFINITION

Remote Desktop Protocol (RDP) is a proprietary network protocol that allows

Alaskan attack surface: RDP

Mitigations (straight from [the FBI recommendations](#))

- Rolling audit of your external network for remote RDP
- Verify need for any public RDP; disable if not needed
- Put RDP behind a firewall and require VPN
 - ... but VPNs are only as secure as connected devices!
- Use strong passwords, account lockout policies
- Apply two-factor authentication
- Apply system and software updates regularly
- Maintain a good backup strategy
- Enable logging for RDP; keep for 90 days; review/alert
- Take special care with critical devices

Alaskan attack surface: SSH

Risks

- Password-only SSH is vulnerable to key logging
- SSH on appliances may be harder to keep patched
- False positives in vulnerability detection
(due to silent backporting of fixes w/o updating version string)

Alaskan attack surface: SSH

Scope

- Dropbear: 909
- OpenSSH family:
 - generic : 557; FIPS: 11
- Ubuntu/Debian/Raspbian: 226
- HipServ (Axentra/NETGEAR/GoFlex): 91
- Cisco (or related WLC): 246
- ROSSH (RouterOS): 102
- FreeBSD: 25
- Mocana (NanoSSH): 15
- Juniper NetScreen: 8
- FTP (CoreFTP, Cerberus): 7

Alaskan attack surface: SSH

Mitigations

- Geofence: North America, [Alaskan nets](#), bastion hosts?
- SSH keys (instead of just passwords alone)
- Log authentication success and failure
(especially if exposed public SSH is unexpected)
- Use [fail2ban](#) and similar throttling/blocking mechanisms
- Enable simple MFA (search for “SSH” “PAM” “TOTP”)

```
$ ssh -p [REDACTED]  
Password:  
Verification code:
```

Alaskan attack surface: SSH

Mitigation: PAM-based two-factor (TOTP)

```
$ sudo apt install libpam-google-authenticator
[...]
$ cd /etc/pam.d
$ diff -u sshd-dist sshd
@include common-password
+auth [success=1 default=ignore] pam_access.so \
    accessfile=/usr/local/etc/access-local.conf
+auth required pam_google_authenticator.so nullok
```

```
$ cat /usr/local/etc/access-local.conf
# Only allow from local IP ranges.
+ : ALL : xxx.xxx.xxx.0/24
+ : ALL : LOCAL
- : ALL : ALL
```

Alaskan attack surface: VPN

Risks

- Assuming that VPN must be exposed to *entire* Internet?
Shadow Brokers **BENIGNCERTAIN** says otherwise
- VPN connections sometimes allowed *full* network access
- Security of any reachable networks is only as good as the security of the *worst* VPN-connected endpoint

Alaskan attack surface: VPN

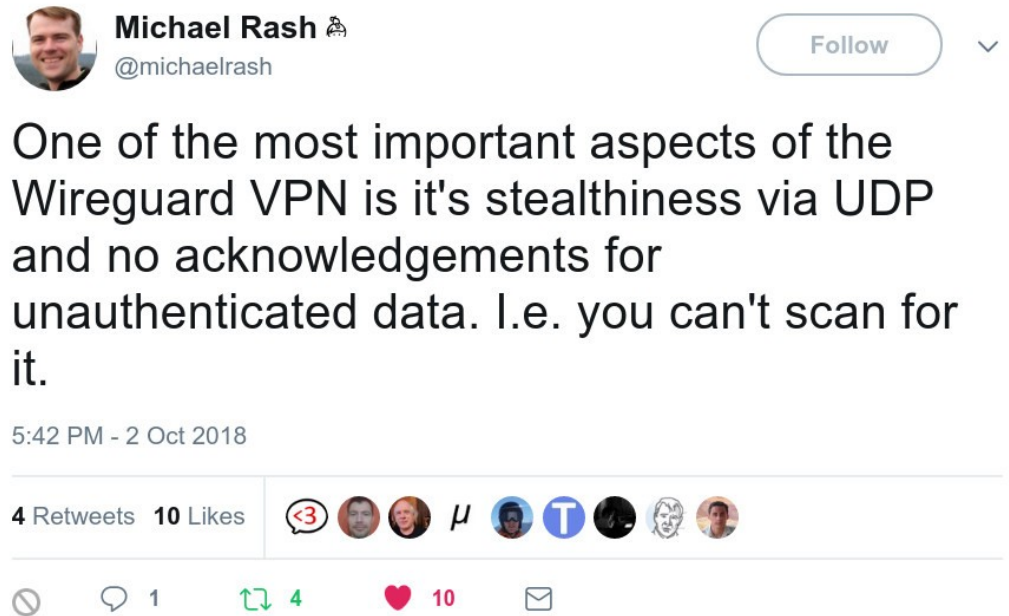
Mitigations

- Logging of auth success & failure is obviously key
- Consider reducing need for VPN for light remote workers
 - Only email and Office 365, etc.
- Consider geofencing or inverted geofencing
 - countries to allow, or at least countries to block
- Make vigorous use of internal segmentation & ACLs
 - limit most VPN clients to minimal subset of network
 - monitor VPN netflows to spot anomalies
- IPS/NGFW in front of VPN if you can get away with it
- See also [US-CERT TA16-250A](#) guidance

Alaskan attack surface: VPN

Mitigations

- Long term:
... consider **WireGuard**:
(self-hosted VPN stack -
even for IR/backup!)
- Near-instant cloud setup:
GitHub [trailofbits/algo](https://github.com/trailofbits/algo)
- An interesting new
alternative: [Outline](#)
(from Jigsaw - Alphabet/Google's "security ecosystem" arm)



Alaskan attack surface: VPN

```
Date: Thu, 2 Aug 2018 10:15:40 -0700
From: Linus Torvalds <torvalds@...ux-foundation.org>
To: David Miller <davem@...emloft.net>
Cc: Andrew Morton <akpm@...ux-foundation.org>,
    Network Development <netdev@...r.kernel.org>,
    Linux Kernel Mailing List <linux-kernel@...r.kernel.org>
Subject: Re: [GIT] Networking

On Wed, Aug 1, 2018 at 9:37 PM David Miller <davem@...emloft.net> wrote:
>
> Fixes keep trickling in:

Pulled.

Btw, on an unrelated issue: I see that Jason actually made the pull
request to have wireguard included in the kernel.

Can I just once again state my love for it and hope it gets merged
soon? Maybe the code isn't perfect, but I've skimmed it, and compared
to the horrors that are OpenVPN and IPSec, it's a work of art.

Linus
```

Alaskan attack surface: VPN

Mitigations

Longer term:

- Start moving **now** towards **Zero Trust** - significant lead time
- By the time you realize you need Zero Trust, you will wish you had started years prior
- Plant that tree **now**

Alaskan attack surface: hostnames

<https://www.techsolvency.com/alaskan-domains-list/>

Current count: 9421 domains
27,113 “interesting” hostnames

Sources:

DNS from Rapid7 Internet-wide scans

Lists of Alaskan websites

Google searches by industry

Reverse DNS from Alaskan IP scans

FQDNs shown in certificate names in Alaskan IP space

Alaskan attack surface: TLS

Public-facing SSL/TLS (443 only)

- 27,112 hostnames potentially using TLS
- **16,228** appear to be using TLS on purpose
- *These numbers shift daily*

Alaskan attack surface: TLS

Of **16,228** TLS-speaking hostnames:

Qualys SSL Labs grades:

- **A+** 487; **A** 5878; **B** 2480; **C** 917; **F**: 1730
- Valid enough to score: 11499
- Entirely untrusted: **4806**

Modern features:

- **HTTP Strict Transport Security (HSTS)**: 1606
- **Forward Secrecy**: all: 6978; modern: 4765; none: **799**

CAs: **common**: 14579; **rare** (self-signed, etc): 1461

- Let's Encrypt: 4542

Alaskan attack surface: TLS

Of **16,228** TLS-speaking hostnames:

Obsolete SSL/TLS protocols:

- SSLv2: 970; SSLv3: 2406
- Negotiating RC4 on modern browsers: 125

Vulnerable to:

- POODLE: SSL 1871; TLS 128
- FREAK: 197; DROWN: 162; CRIME: 66
- **Heartbleed: 6**

Alaskan attack surface: TLS

Discovery

- Nmap scans for 443, 8443 ... ?
- Public sources (Shodan, Censys, crt.sh, Rapid7 scans ...)
- Internal inventory/configs

Alaskan attack surface: TLS

Mitigations

Hardening – based on risk/criticality

- Test with Qualys SSL Labs
- Disable SSLv3 and SSLv3 ASAP
- If grade is F due to vulnerabilities, patch ASAP
- If patching is not possible, consider [stunnel](#) proxy
- Harden to the appropriate level of the [Mozilla guidelines](#)

Alaskan attack surface: TLS

Mitigations

- Collect the data for ongoing management of your configs
- **Log** which ciphers are being negotiated by (legit) clients

Apache: [mod_ssl CustomLog](#) + SSL env variables:

```
CustomLog /path/to/log "%t %h %{REMOTE_USER}x  
\"%{User-agent}i\" \ %{SSL_PROTOCOL}x %{SSL_CIPHER}x "
```

- Collect logs for X days (minimum 90?)
- If (non-bot) clients don't need old ciphers, **disable**

The case for undue diligence

The case for ~~undue~~ diligence

Being a good Alaskan neighbor: reducing your *internal* attack surface

The *internal* attack surface

... is just like the external one

- Everything that we've discussed so far ...
... should also be applied to your *internal* network
- You **must** start seeing what an attacker can see
- Start simple, focusing on *visibility* first
- Collect the *minimum* data necessary to *inform next steps*
- Initiate plans for standing up a true internal Red Team

The *internal* attack surface

The endpoint: fast Windows tips

- Map .vbs, .wsh, .js, etc. to Notepad
- Use local hosts file to blackhole ad networks (mvps.org)
- Microsoft [LAPS](#) (unique local admin passwords), [PAWs](#)
- [Sysmon](#) (Microsoft Sysinternals)
- + [SwiftOnSecurity](#)'s [sysmon-config](#) starter kit
- Microsoft [Windows Event Forwarding](#) (“WEF”)
(Instead of pulling logs over slow WAN, filter at endpoint!)
- Bonus: solid list of Windows refresh/clean/unbreak tips:
<https://decentsecurity.com/holiday-tasks/> (SwiftOnSecurity)

The *internal* attack surface

More fast Windows tips – pentest/ransomware killchain

- Segment unpatchable MS systems
 - jumpbox access only, ACL/firewall, etc
- Decouple Domain Admins from local logon rights
- Reduce/isolate SMBv1 (MS “[Product Clearinghouse](#)”)
 - or selectively enable only where needed
- Microsoft [Device Guard and Credential Guard](#)

The *internal* attack surface

Fast general tips – pentest/ransomware killchain

- Semi-targeted ransomware will make a bee-line for your backups
- If your backups aren't offline to you, they're not offline for an attacker who has stolen your credentials

The *internal* attack surface

WIRED

The Untold Story of NotPetya, the Most Devastating

SIGN IN | SI

After a frantic global search, the admins finally found one lone surviving domain controller in a remote office—in Ghana.

After a frantic search that entailed calling hundreds of IT admins in data centers around the world, Maersk's desperate administrators finally found one lone surviving domain controller in a remote office—in Ghana. At some point before NotPetya struck, a blackout had knocked the Ghanaian machine offline, and the computer remained disconnected from the

network. It thus contained the singular known copy of the company's domain controller data left untouched by the malware—all thanks to a power outage. "There were a lot of joyous whoops in the office when we found it," a Maersk administrator says.

Source: [Wired](#)

The *internal* attack surface

The browser: fast Chrome tips

The *internal* attack surface

The browser: fast Chrome tips

Extensions:

- [uBlock Origin](#) and [uBlock Origin Extra](#) (Raymond Gorhill)
- [HTTPS Everywhere](#) (EFF)
- [Privacy Badger](#) (EFF)
- Enable “Prevent WebRTC from leaking local IP address”
- Not recommended: Adblock, Adblock Plus, Ghostery (potential conflicts of interest)
- Watch the supply chain (extension owners)

The *internal* attack surface

The browser: fast Chrome tips

- Flags (`chrome://flags`):
- Strict site isolation – *enabled*
- Extension Content Verification – *enforce strict*
- Reduce default 'referrer' header granularity - *enabled*
- Framebusting requires same-origin or a user gesture - *enabled*
- Fill passwords on account selection - *enabled*
- Block tab-unders - *enabled*
- PDF isolation - *enable*
- Omnibox UI Hide URL Scheme / Trivial Subdomains - *disable for geeks*

Test in your environment. YMMV.

The *internal* attack surface

The browser: fast Chrome tips

Other tips:

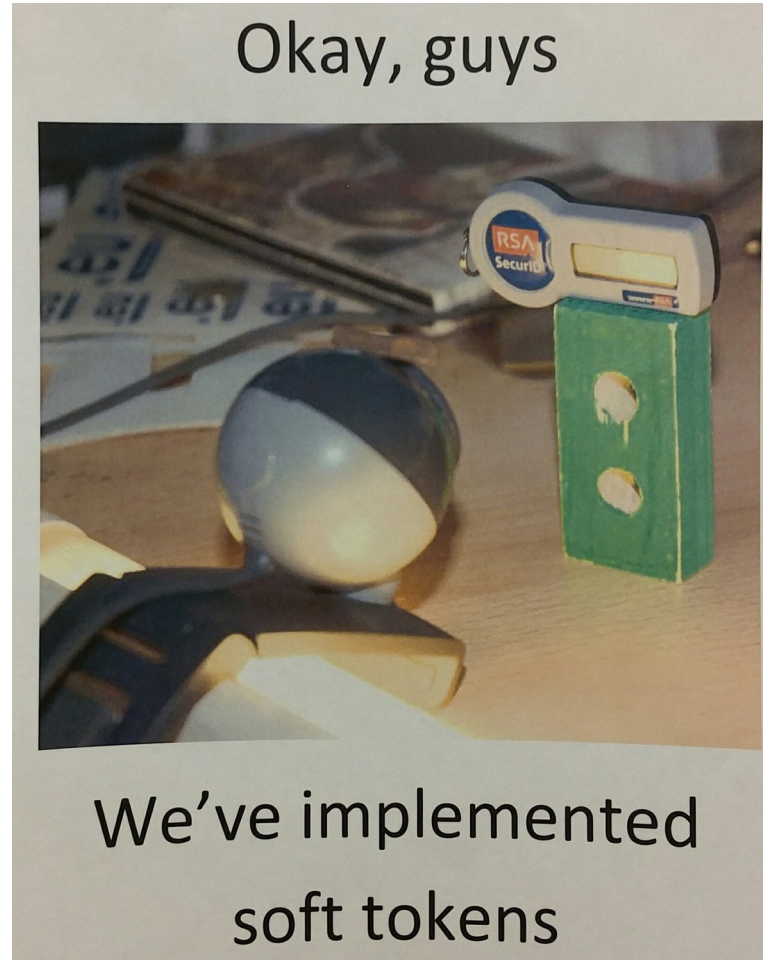
- Switch to [Chrome Enterprise](#) – GPO-driven
- Allow Chrome auto-update on remote or high-risk endpoints
- Let IT and web teams also run Chrome “beta” and “dev”
- Consider moving to Chrome as *primary* PDF viewer (or keeping it ready if there is a 0-day in your primary)
- See also TechRepublic [“Tips for the Paranoid at Heart”](#)

The *internal* attack surface

Other tips (apply based on risk)

- Enable UAC. Seriously.
- Use full-disk encryption - for *anything someone can carry*
- Wipe *everything* before it leaves your environment
See <https://www.techsolvency.com/pub/bin/erasing-storage/>
- Turn on MFA for any supporting platform
 - Yes, SMS sucks – but *it sucks less than no 2FA at all*
- If you can afford hard tokens, use them for high-value targets (Domain Admins, executives ...)
- A soft token is software on a small unpatched pocket computer

The *internal* attack surface



Self-assessment: key self-managed tools

(for internal and external use)

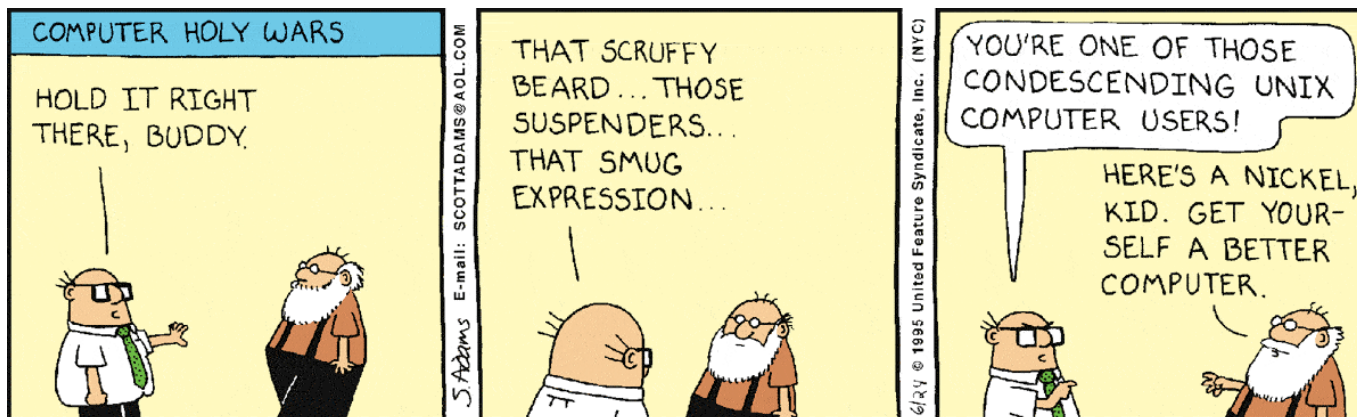
Masscan

Nmap

DMARC

testssl.sh

Vuln scanners (or **OpenVAS**) as discovery engines



Self-assessment: key self-managed tools

Masscan

```
Starting masscan 1.0.6 (http://bit.ly/14GZzcT) at 2018-10-01 05:19:21 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 751104 hosts [24 ports/host]
Rate: 9.96-kpps, 0.88% done, 0:29:20 remaining, found=333
```

Best intro: [Masscan Primer by Daniel Miessler](#)

Self-assessment: key self-managed tools

Nmap

- Basic usage should already be familiar – if not, *fix that*
- The Nmap Scripting Engine (NSE) is a **key** IR tool
- Breaking news about 0-days is almost always immediately followed by the release of NSE-based detection scripts – often before they appear in commercial scanners
- Speed tip: feed IPs from masscan to nmap!

Self-assessment: key self-managed tools

testssl.sh

- Stand-alone bash script
- Reports many of the same issues as Qualys SSL Labs ... but you can run it *internally*
- Includes the statically compiled ancient SSL needed to detect old ciphers

```
dirks@laptop:~/git.testssl.sh$ ./testssl.sh dev.testssl.sh
#####
testssl.sh      2.6 from https://testssl.sh/
(58096d6 2015-09-15 08:49:00 -- 1.379)

This program is free software. Distribution and
modification under GPLv2 permitted.
USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

Please file bugs @ https://testssl.sh/bugs/

#####

Using "OpenSSL 1.0.2-chacha (1.0.2d-dev)" ["181 ciphers] on
trex:*PWD/bin/openssl.Linux.x86_64
(built: "Jul  6 18:05:33 2015", platform: "linux-x86_64")

Testing now (2015-09-15 22:41) --> 81.169.199.25:443 (dev.testssl.sh) <---

rDNS (81.169.199.25):  testssl.sh.
Service detected:      HTTP

--> Testing protocols (via sockets except TLS 1.2 and SPDY/NPN)

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      offered
TLS 1.1    offered
TLS 1.2    offered (OK)
SPDY/NPN   http/1.1 (advertised)

--> Testing ~standard cipher lists

Null Ciphers      not offered (OK)
Anonymous NULL Ciphers offered (NOT ok)
Anonymous DH Ciphers offered (NOT ok)
40 Bit encryption offered (NOT ok)
56 Bit encryption not offered (OK)
Export Ciphers (general) offered (NOT ok)
Low (<=64 Bit)    not offered (OK)
DES Ciphers       not offered (OK)
Medium grade encryption offered (NOT ok)
Triple DES Ciphers offered (NOT ok)
High grade encryption not offered (NOT ok)

--> Testing (perfect) forward secrecy, (P)FS -- omitting 3DES, RC4 and Null E

PFS is offered (OK) DHE-RSA-SEED-SHA ECDHE-RSA-RC4-SHA
```

Self-assessment: key self-managed tools

DMARC - Value

- Simple to set up – just a DNS record and a mailbox
- Reduce **or even eliminate** email spoofed from your domain to major email providers – *in a controlled and gradual manner*
- Near-instant email visibility out of the box

Self-assessment: key self-managed tools

DMARC - Method

- Set up DNS records
- Set up an email mailbox to handle incoming reports
 - Tip: for best results, *use one in the target domain*
- Find a script to process incoming emailed reports (JSON)
 - I adapted a Yahoo script for CSV output, available [here](#)
- Start in “report only mode” (`p=none`)
- When ready, change to `p=quarantine`; analyze
- Move to `p=reject` (if and when you choose or need to)

Self-assessment: key self-managed tools

DMARC - example

```
$ host -t txt _dmarc.pl8.com
```

```
_dmarc.pl8.com descriptive text
```

```
"v=DMARC1; p=reject;  
rua=mailto:postmaster@pl8.com;  
ruf=mailto:postmaster@pl8.com; fo=1; aspf=r"
```

org_name	date_begin	date_end	domain	p	source_IP	dispos	header_from	spf_dom	spf_res
Google	2018-09-04	2018-09-05	pl8.com	none	[Unicom-CN]	none	pl8.com	pl8.com	neutral
126.com	2018-09-04	2018-09-05	pl8.com	none	[Huashu-CN]	none	pl8.com	pl8.com	neutral
Google	2018-09-05	2018-09-06	pl8.com	none	[Unicom-CN]	none	pl8.com	pl8.com	neutral
Google	2018-09-05	2018-09-06	pl8.com	none	[Unicom-CN]	none	pl8.com	pl8.com	neutral
Google	2018-09-05	2018-09-06	pl8.com	none	[Huashu-CN]	none	pl8.com	pl8.com	neutral
Google	2018-09-05	2018-09-06	pl8.com	none	[Mobile-CN]	none	pl8.com	pl8.com	neutral
126.com	2018-09-05	2018-09-06	pl8.com	none	[ChinaNet]	none	PL8.com	pl8.com	neutral
Google	2018-09-06	2018-09-07	pl8.com	none	[Unicom-CN]	none	pl8.com	pl8.com	neutral
126.com	2018-09-08	2018-09-09	pl8.com	none	[ChinaNet]	none	PL8.com	pl8.com	neutral
Google	2018-09-09	2018-09-10	pl8.com	none	[Unicom-CN]	none	pl8.com	pl8.com	neutral
Google	2018-09-14	2018-09-15	pl8.com	reject	[Mobile-CN]	reject	pl8.com	pl8.com	fail
Google	2018-09-14	2018-09-15	pl8.com	reject	[Huashu-CN]	reject	pl8.com	pl8.com	fail
Google	2018-09-15	2018-09-16	pl8.com	reject	[Unicom-CN]	reject	pl8.com	pl8.com	fail
Google	2018-09-15	2018-09-16	pl8.com	reject	[Unicom-CN]	reject	pl8.com	pl8.com	fail
Yeah	2018-09-15	2018-09-16	pl8.com	reject	[Unicom-CN]	none	pl8.com	pl8.com	neutral
Google	2018-09-16	2018-09-17	pl8.com	reject	[Mobile-CN]	reject	pl8.com	pl8.com	fail
Google	2018-09-16	2018-09-17	pl8.com	reject	[Unicom-CN]	reject	pl8.com	pl8.com	fail
Mail.Ru	2018-09-20	2018-09-21	pl8.com	reject	195.202.55.242	reject	pl8.com	pl8.com	fail
Google	2018-09-26	2018-09-27	pl8.com	reject	192.3.141.3	reject	pl8.com	dsfdsfc54.net	none
163.com	2018-10-02	2018-10-03	pl8.com	reject	182.38.32.156	none	pL8.com	pl8.com	neutral

Until DMARC, I had ***no idea*** that Chinese spammers spoof mail from **pl8.com**!

Self-assessment: key self-managed tools

Nmap

- Basic usage should already be familiar – if not, *fix that*
- The Nmap Scripting Engine (NSE) is a **key** IR tool
- Breaking news about 0-days is almost always immediately followed by the release of NSE-based detection scripts – often before they appear in commercial scanners
- Speed tip: feed IPs from masscan to nmap!

Self-assessment: key concepts

First stage: inventory and discovery

Second stage: triage, goal-setting, and retrofit

Third stage: validate and monitor over time

Self-assessment: key external tools

Overall

[Hardenize](#) - best of the best

TLS

[Qualys SSL Labs Server Test](#)

[Nartac "IIS Crypto"](#) - easy hardening of IIS TLS

[crt.sh](#) – easy search of Certificate Transparency logs

HTTP headers

[SecurityHeaders.com](#)

External attack surface

[Shodan](#), [Censys](#)

Domain hardening: Hardenize

Hardenize HOME PRODUCT DASHBOARDS BLOG ABOUT | AC

Public Report | techsolvency.com TEST AND

techsolvency.com
29 Sep 2018 23:32 UTC [Tweet](#)

Domain

- ✓ Name servers
- ✓ DNSSEC
- ✓ CAA

Email

- ✓ Mail servers
- SECURE TRANSPORT (SMTP)
- ✓ TLS
- ✓ Certificates
- ✗ MTA-STS
- ✗ DANE

WEB SECURITY OVERVIEW

✓ HTTPS
Web sites need to use encryption to help their visitors know they're in the right place, as well as provide confidentiality and content integrity. Sites that don't support HTTPS may expose sensitive data and have their pages modified and subverted.

For all sites
VERY IMPORTANT
MEDIUM EFFORT


✓ HTTPS Redirection
To deploy HTTPS properly, web sites must redirect all unsafe (plaintext) traffic to the encrypted variant. This approach ensures that no sensitive data is exposed and that further security technologies can be activated.

For all sites
VERY IMPORTANT
LOW EFFORT

✓ HTTP Strict Transport Security
HTTP Strict Transport Security (HSTS) is an HTTPS extension that instructs browsers to remember sites that use encryption and enforce strict security

For important site
VERY IMPORTANT

Domain hardening: Hardenize



SITES

CERTIFICATES

CT

CRTDB

WORKBENCH

ACCOUNT

SETTINGS

Q *.example.com

Columns Filter: All Sort by: Hostname

	DOMAIN	EMAIL	WWW									
Hostname	Name servers	DNSSEC	TLS	DANE	SPF	DMARC	TLS	Cookies	Mixed content	HSTS	CSP	Security headers
	✓	-	⚠	-	✓	-	✓	✓	✓	-	-	-
	✓	-	✓	-	✓	-	!	✓	✓	-	-	-
	✓	-	!	-	✓	-	!	✓	✓	-	-	-
	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓	✓
	✓	-	-	-	✓	-	✓	⚠	✓	-	-	-
	✓	-	⚠	-	✓	✓	✓	✓	✓	✓	-	-
	✓	-	⚠	-	✓	-	✓	✓	✓	✓	✓	✓
	✓	-	-	-	-	-	✓	✓	✓	-	-	-

TLS hardening: Qualys SSL Labs Server Test

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > akmon.techsolvency.com

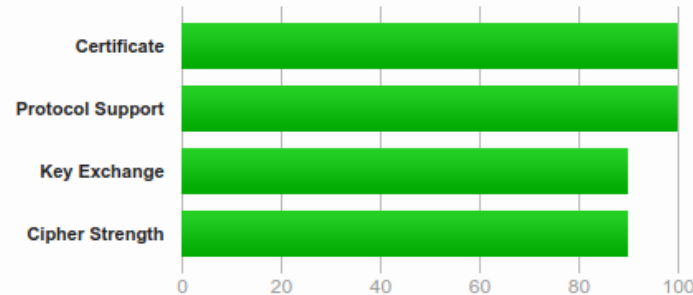
SSL Report: akmon.techsolvency.com (104.131.148.95)

Assessed on: Tue, 02 Oct 2018 05:15:56 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

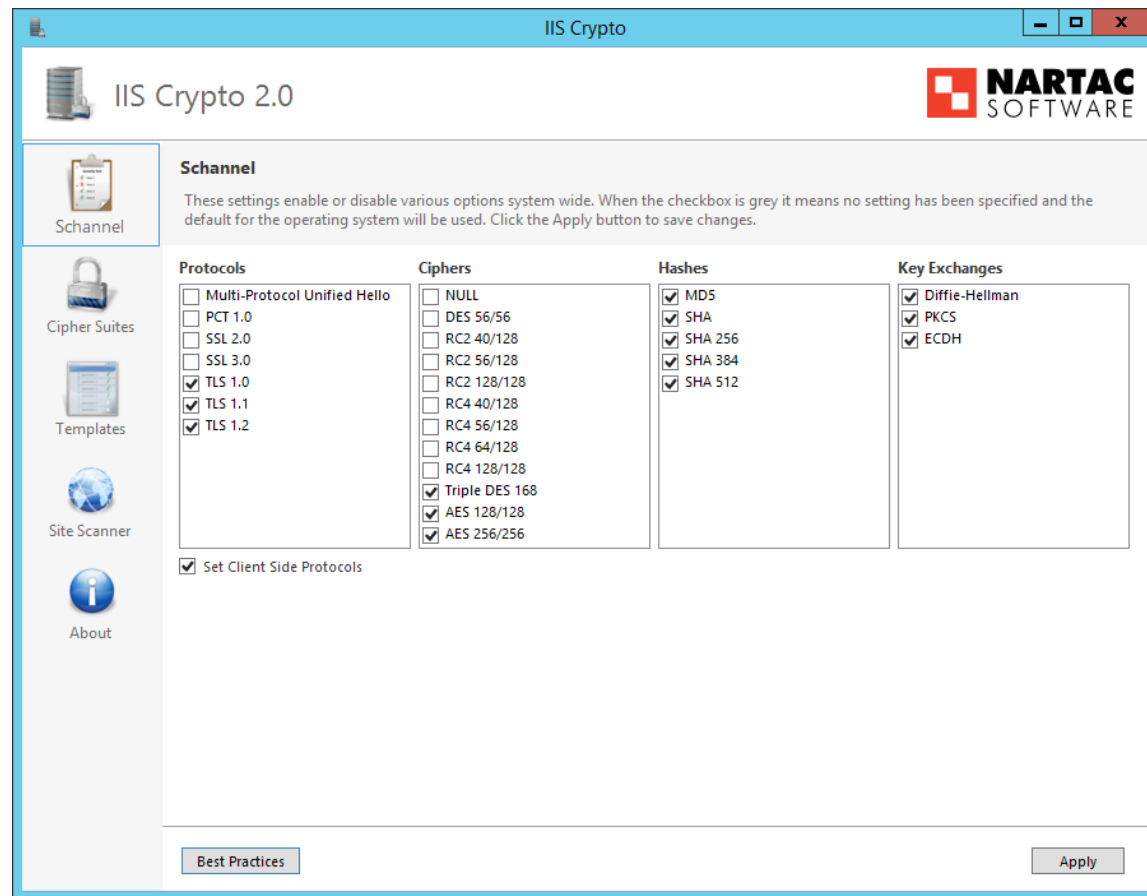
HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

TLS hardening (IIS): Nartac IISCrypto

Value: simple GUI with sets of baseline defaults, fixes most IIS TLS issues fast

... instead of registry changes



TLS visibility: crt.sh



Enter an **Identity** (Domain Name, Organization Name, etc),
a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**:

(% = wildcard)

%.techsolvency.com

Search

[Advanced...](#)

TLS visibility: crt.sh



Identity Search



[Group by Issuer](#)

Criteria

Identity LIKE '%.techsolvency.com'

crt.sh ID	Logged At ↑	Not Before	Not After	Identity	Issuer Name
794342533	2018-09-28	2018-09-28	2018-12-27	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
805489044	2018-09-18	2018-09-15	2018-12-14	www.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
751240986	2018-09-15	2018-09-15	2018-12-14	www.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
805489023	2018-09-06	2018-09-06	2018-12-05	akmon3.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
721297879	2018-09-06	2018-09-06	2018-12-05	akmon3.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
675957039	2018-07-30	2018-07-30	2018-10-28	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
654244406	2018-07-30	2018-07-30	2018-10-28	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
628715550	2018-07-17	2018-07-17	2018-10-15	www.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
604528549	2018-07-17	2018-07-17	2018-10-15	www.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
596291365	2018-07-08	2018-07-08	2018-10-06	akmon3.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
581929945	2018-07-08	2018-07-08	2018-10-06	akmon3.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
486543028	2018-05-25	2018-05-25	2018-08-23	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
485516272	2018-05-25	2018-05-25	2018-08-23	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
470143117	2018-05-18	2018-05-18	2018-08-16	www.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
470142726	2018-05-18	2018-05-18	2018-08-16	www.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
452813407	2018-05-09	2018-05-09	2018-08-07	akmon3.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
450559060	2018-05-09	2018-05-09	2018-08-07	akmon3.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
366538261	2018-03-26	2018-03-26	2018-06-24	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
358842099	2018-03-18	2018-03-18	2018-06-16	www.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
310788930	2018-01-22	2018-01-22	2018-04-22	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
259774796	2017-11-20	2017-11-20	2018-02-18	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
212701158	2017-09-18	2017-09-18	2017-12-17	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
174087846	2017-07-17	2017-07-17	2017-10-15	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
137276114	2017-05-13	2017-05-13	2017-08-11	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
99044385	2017-03-04	2017-03-04	2017-06-02	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
70333456	2016-12-24	2016-12-24	2017-03-24	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
43976723	2016-10-15	2016-10-15	2017-01-13	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
27074630	2016-08-06	2016-08-06	2016-11-04	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
20386096	2016-05-28	2016-05-28	2016-08-26	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
14885524	2016-03-09	2016-03-08	2016-06-06	akmon.techsolvency.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1

HTTP header checks: SecurityHeaders.com

Value

- See how your sites are controlling XSS, frames, etc.
 - Stay off the “free pentest” radar

HTTP header checks: SecurityHeaders.com

☐ Hide results ☐ Follow redirects

Security Report Summary



Site: <https://www.techsolvency.com/>

IP Address: 216.92.135.245

Report Time: 04 Oct 2018 14:09:29 UTC

Headers:

- ✓ Strict-Transport-Security
- ✓ Content-Security-Policy
- ✓ Feature-Policy
- ✓ Referrer-Policy
- ✓ X-Content-Type-Options
- ✓ X-Frame-Options
- ✓ X-XSS-Protection

Raw Headers

HTTP/1.1	200 OK
Date	Thu, 04 Oct 2018 14:09:29 GMT
Server	Apache/2.4.35
Strict-Transport-Security	max-age=31589246; IncludeSubDomains; preload
Last-Modified	Sun, 30 Sep 2018 03:08:44 GMT

Website control: Content Security Policy

Value

*Control what third parties can change on your sites
– **or inject into them***

Website control: Content Security Policy

Method

- A multi-part HTTP header
- Specifies fine-grained control of site resources
- More precise and flexible than older security headers
- Sends you reports **from client browsers**

Website control: Content Security Policy

Simple example: (eBay):

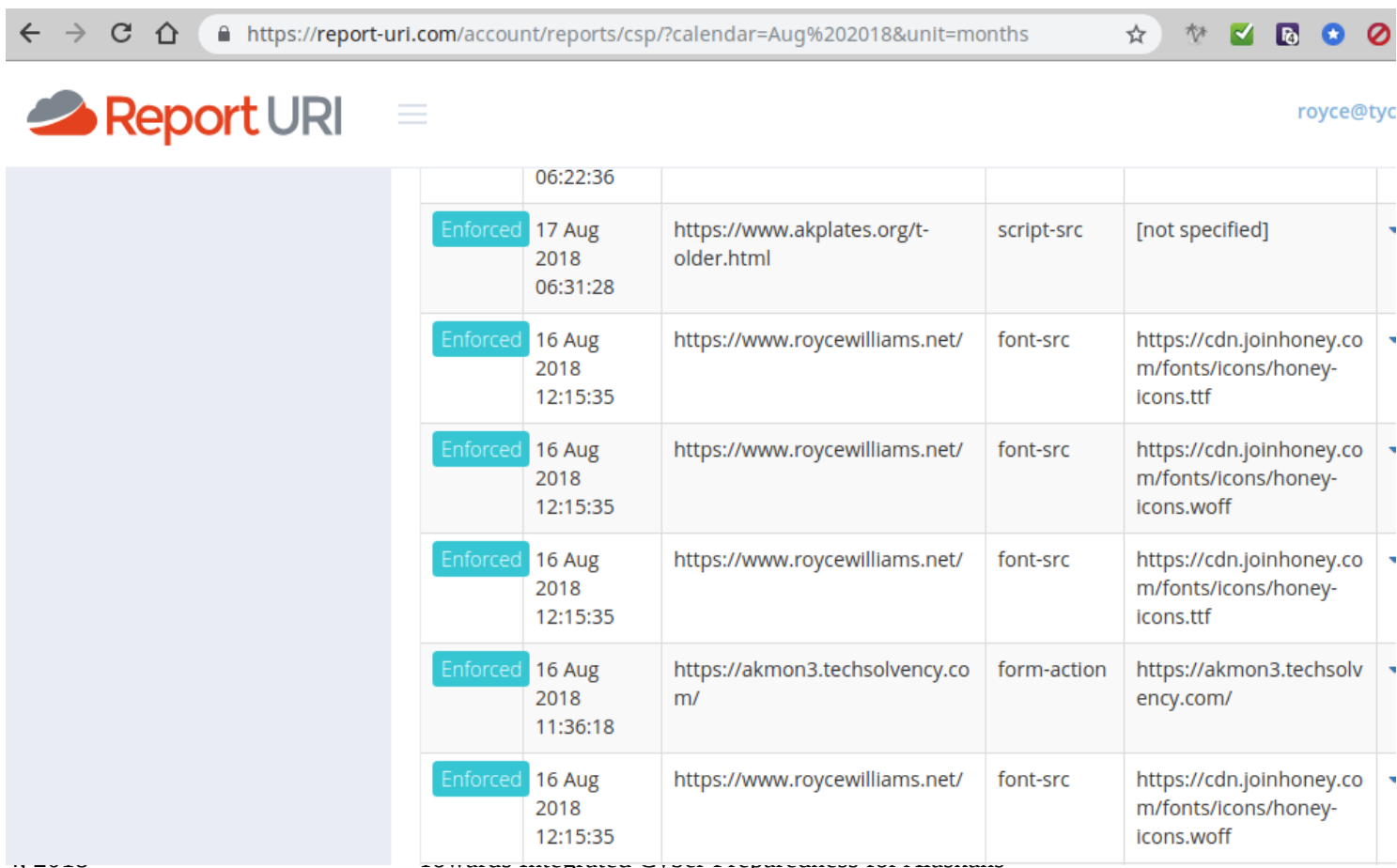
```
Content-Security-Policy: default-src 'self' blob: wss: data: https;; img-src 'self' data: https;; script-src 'self' 'unsafe-eval' 'unsafe-inline' blob: data: https;; style-src 'self' 'unsafe-inline' data: https;;
```

More complex example (techsolvency.com):

```
Content-Security-Policy: default-src 'none'; script-src 'self' https://www.googletagmanager.com https://www.google-analytics.com; connect-src 'self' https://www.google-analytics.com; img-src 'self' https://www.googletagmanager.com https://www.google-analytics.com https://jigsaw.w3.org https://www.w3.org; style-src 'self'; font-src 'self'; object-src 'none'; frame-src 'none'; frame-ancestors 'none'; base-uri 'self'; form-action 'self'; block-all-mixed-content; require-sri-for script; report-uri https://techsolvency.report-uri.com/r/d/csp/enforce;
```

Website control: Content Security Policy

Verify and monitor with tools like Report URI:



The screenshot shows a web browser window with the address bar displaying `https://report-uri.com/account/reports/csp/?calendar=Aug%202018&unit=months`. The page header includes the "Report URI" logo and the user email "royce@tyc". A large grey sidebar is on the left. The main content area displays a table of CSP violations.

	06:22:36				
Enforced	17 Aug 2018 06:31:28	https://www.akplates.org/t-older.html	script-src	[not specified]	
Enforced	16 Aug 2018 12:15:35	https://www.roycewilliams.net/	font-src	https://cdn.joinhoney.com/fonts/icons/honey-icons.ttf	
Enforced	16 Aug 2018 12:15:35	https://www.roycewilliams.net/	font-src	https://cdn.joinhoney.com/fonts/icons/honey-icons.woff	
Enforced	16 Aug 2018 12:15:35	https://www.roycewilliams.net/	font-src	https://cdn.joinhoney.com/fonts/icons/honey-icons.ttf	
Enforced	16 Aug 2018 11:36:18	https://akmon3.techsolvency.com/	form-action	https://akmon3.techsolvency.com/	
Enforced	16 Aug 2018 12:15:35	https://www.roycewilliams.net/	font-src	https://cdn.joinhoney.com/fonts/icons/honey-icons.woff	

Easing into Content Security Policy (CSP)

- Use Content-Security-Policy-**Report-Only** first
- Localize what you can
 - most remote components (jQuery, etc.)
 - remote webfonts
- Add a checksum if you can't
 - Prevents CDN code hijacking (Newegg)
- Simplify and modernize your links
 - Easy: Change old outbound HTTP to HTTPS
 - Medium: Reduce mixed HTTP/HTTPS content
 - Harder: reduce inline scripts and styles
- Do this based on risk (login pages, etc.)

Assessing browser support

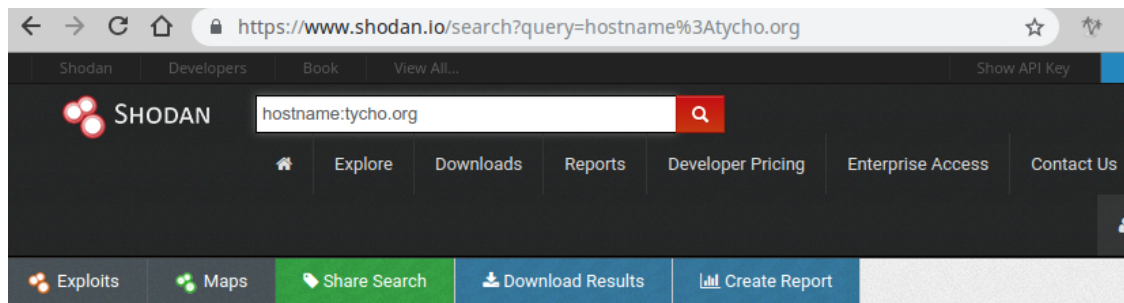
Use
caniuse.com
to check
which browsers
support your
target features



Attack surface checks: Shodan Value

See what the attacker can see – at scale

Attack surface checks: Shodan.io



TOTAL RESULTS

71,105

TOP COUNTRIES



United States

71,105

TOP SERVICES

HTTP	14,318
HTTPS	8,078
NTP	3,611
HTTP (8080)	3,555
SSH	1,648

TOTAL RESULTS

8

TOP COUNTRIES



United States 8

TOP SERVICES

SSH	3
HTTPS	2
HTTP	2
IKE	1

TOP ORGANIZATIONS

Digital Ocean	5
pair Networks	3

TOP PRODUCTS

165.227.13.43

velo.tycho.org

Digital Ocean

Added on 2018-09-30 09:42:16 GMT

United States, New York

Details

vpn cloud

VPN (IKE)

Initiator SPI: 63716c6776627379

Responder SPI: 68336476796e6567

Next Payload: RESERVED

Version: 2.0

Exchange Type: DOI Specific Use

Flags:

Encryption: False

Commit: False

Authentication: False

Message ID: 00000000

Length: 36

Alaskan infrastructure monitoring - Tech Solvency

104.131.148.95

leo.tycho.org

Digital Ocean

Added on 2018-09-29 13:51:50 GMT

United States, New York

Details

cloud

SSL Certificate

Issued By:

|- Common Name: Let's Encrypt

Authority X3

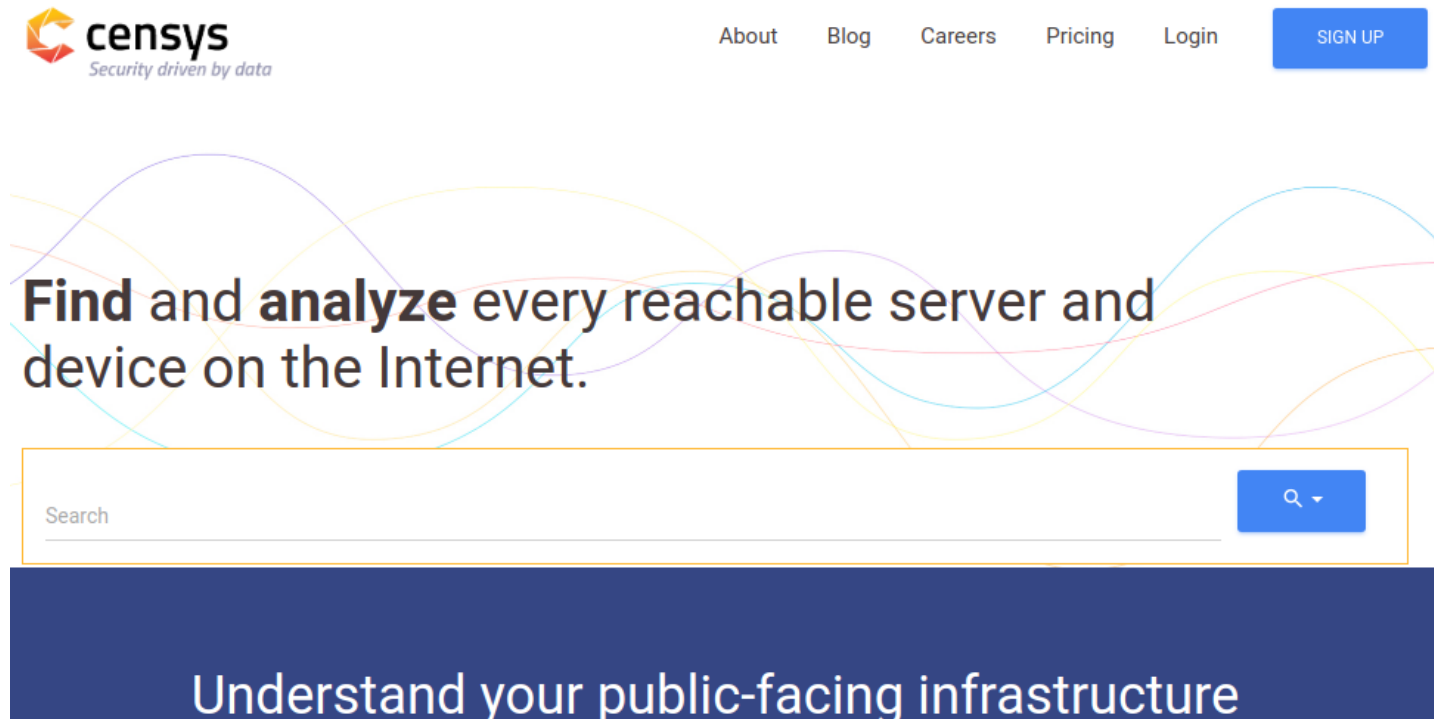
|- Organization: Let's Encrypt

Issued To:

|- Common Name:

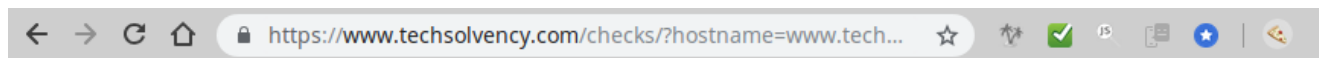
akmon.techsolvency.com

Attack surface checks: Censys.io



- Also consider downloading the raw DNS datasets
<https://registry.opendata.aws/rapid7-fdns-any/>

Cheat sheet: [techsolvency.com/checks](https://www.techsolvency.com/checks)



[Tech Solvency](#) / [Checks](#) / [www.techsolvency.com](#)

Site-checking tools - for security, validity, and usability

Given a fully-qualified hostname, this form generates links to multiple site-checking tools. (Some tools prefer bare domains, so we will attempt to extract the domain - or you can specify one). Tools in **bold** are essential. In most tools that provide a score or rating, red warrants short-term attention.

Enter your hostname below to generate custom links to each tool:

Hostname:

Domain (optional):

(or [start over](#))

On smaller screens, the 'Description and notes' column is hidden.

Tool links for hostname: [www.techsolvency.com](#)

(and potential links to site itself (not verified): [HTTP](#) and [HTTPS](#))

Category	Tool	Custom link to tool	Description and notes
Attack surface	Shodan *	techsolvency.com	Internet-wide IP / service scans. Requires free login for hostname search - definitely worth it.

Cheat sheet: techsolvency.com/checks

Tool links for hostname: www.techsolvency.com

(and potential links to site itself (not verified): [HTTP](http://techsolvency.com) and [HTTPS](https://techsolvency.com))

Category	Tool	Custom link to tool	Description and notes
Attack surface	Shodan *	techsolvency.com	Internet-wide IP / service scans. Requires free login for hostname search - definitely worth it.
Attack surface	Censys *	techsolvency.com	Internet-wide IP / service scans. Be sure to check the 'IPv4', 'website', and 'certificates' sections. Eventually requires free login (after a certain number of queries per day).
Attack surface	DNS Dumpster	(use direct link)	DNS and recon data, based on Censys and Rapid7 Internet-wide IP / service scans - but often has unique analysis and discovered hosts.
Attack surface	RiskIQ Community Edition *	techsolvency.com	Wide variety of correlated public data. Be sure to check each tab. Free login required.
Attack surface	ZoomEye	www.techsolvency.com	The Chinese equivalent of Shodan.
Multi	Hardenize	techsolvency.com	One of the best site security validation suites - includes HTTP TLS, HTTP headers, DNS/DNSSEC, email TLS, email controls (SPF/DKIM/DMARC), and more. Includes very clear explanations and analysis. Once you've assessed

Regional coordination opportunities

Regional coordination opportunities

AKMon – Alaskan regional infrastructure monitoring

<https://www.techsolvency.com/akmon/>

Purpose:

- For the public: Internet performance data for critical infrastructure
- For admins: troubleshooting, performance over time

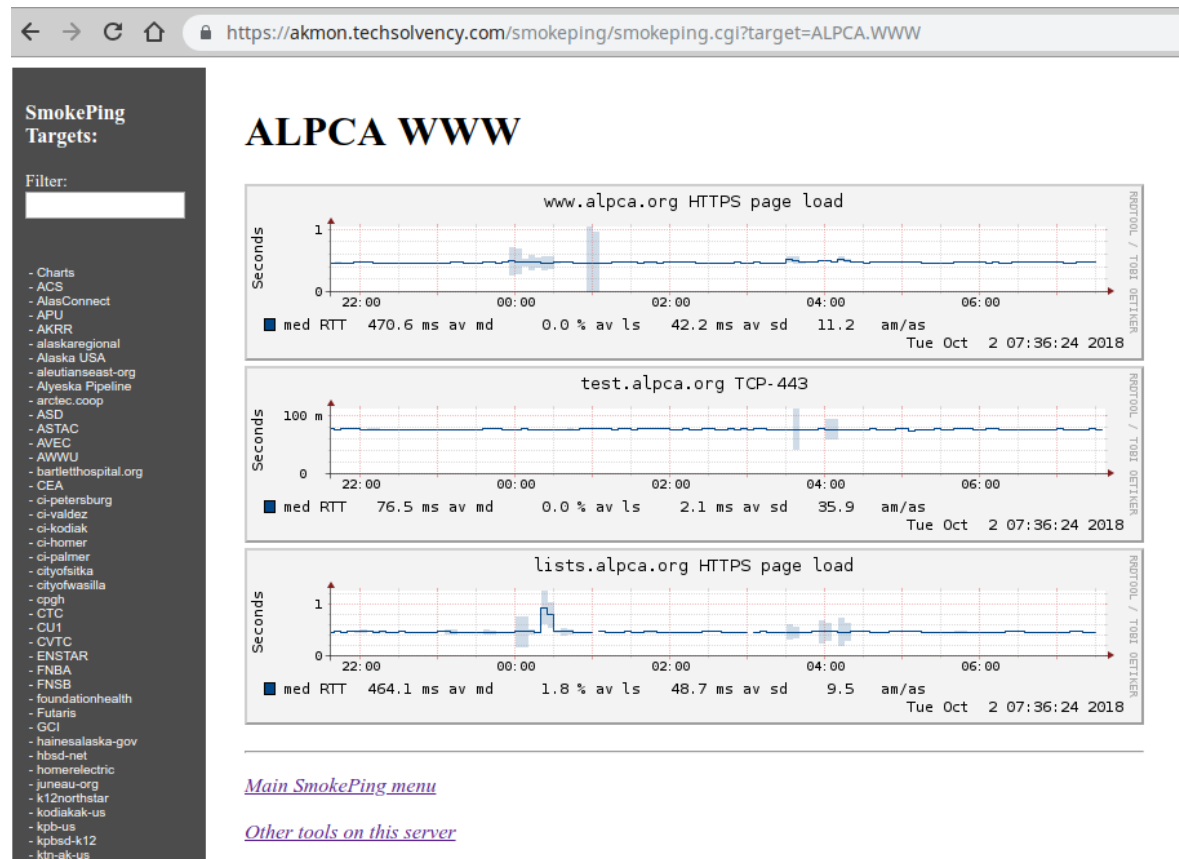
Note:

- Derived **solely** from public (or volunteered) information
- Lacks some obvious areas (defense, food)
- Be aware of the location of polling sources (ANC, SFO)

Regional coordination opportunities

AKMon – Alaskan regional infrastructure monitoring

Currently based
only on Smokeping
(up/down, latency,
packet loss)



Regional coordination opportunities

AKMon – Alaskan regional infrastructure monitoring

ACS	AWWU	CU1	k12northstar	north.slope.org
AlasConnect	bartletthospital.org	CVTC	kodiakak.us	Northrim
APU	CEA	ENSTAR	kpb.us	nwabor.org
AKRR	ci.petersburg	FNBA	kpbsd.k12	OTZ
alaskaregional	ci.valdez	FNSB	ktn.ak.us	SoA
Alaska USA	ci.kodiak	foundationhealth	MEA	TelAlaska
aleutianseast.org	ci.homer	Futaris	matsu.gov	UA
Alyeska Pipeline	ci.palmer	GCI	matsuregional	Unicom
arctec.coop	cityofsitka	hainesalaska.gov	ML&P	whitestone.link
ASD	cityofwasilla	hbsd.net	MTA	wrangell.com
ASTAC	cpgh	homerelectric	Muni ANC	
AVEC	CTC	juneau.org	NANA	

Regional coordination opportunities

Existing communities

ACP

AITP

AKLUG

InfraGard

NUGA

Specialized platform user groups:

Apple, AutoCAD, GIS, ISC², SAS, VMUG

Social: LinkedIn, Facebook, etc.

Regional coordination opportunities

Shared intel?

Sharing of IOCs ([Fast Incident Response](#) Framework)

Coordinated black-holing: DNS, BGP, email
(how to escalate? To who?)

Emergency comms channels in advance:
private distribution lists, Signal groups, IRC?

Regional coordination opportunities

Shared intel?

- * Sharing threat intel with competitors is obviously a delicate matter
 - * But remember: these are also our neighbors
- * In a true regional cyber or mixed event, we will only have each other
- * Give some thought to what level of coordinated response we can set up (and test) in advance

Thanks

agl__	cowboym	FiloSottile	lakiw	munin	spacerog
__agwa	cperciva	gentilkiwi	laparisa	NotMedic	squadgunner
ajstein	cybergone	hdmoore	lhartford	pzb	syzdek
ak_hepcat	dfranke	hillbrad	m33x	rlove	taviso
AlecMuffett	DidierStevens	hydraze	m3g9tr0n	s3in!c	The Dark Tangent
ashk4n	digininja	igrigorik	m8urnett	samykamkar	thorsheim
atom	doc2n	iristic	malcomvetter	Scott_Helme	unix-ninja
atoponce	dwheeler	jenkijp	matthew_d_green	securityerrata	wendyck
attrc	epixoip	JohnLaTwC	mckusick	simestd	winsock32
bmenrigh	erescorla	jschauma	mubix	sleeви_	winxp5421
boblord	ErrataRob	KimZetter	mudge	solardiz	Taylor-MadeAK

Thanks

Take-away links at techsolvency.com/ ...

[/akmon/](#) - Alaskan infra monitoring over time

[/alaskan-networks/](#) - Alaskan IP lists

[/checks/](#) - easy pointers to recommended tests

[/alaskan-domains-list/](#)

[/tls/](#) - TLS health of Alaskan hosts, w/tips & links

[/blue-team/](#) & [/red-team/](#) - many other refs

Contact: royce@techsolvency.com | [@TychoTithonus](#)

(Also follow [@techsolvency](#) - curated “Alaska Cyber Watch” news & commentary)

Slides, errata, and references:

<https://www.techsolvency.com/talks>

