MODUSBOX

Attacking Financial Institutions at Scale

Dispelling myths about how reconnaissance works and why your traditional defenses may mean nothing.

Note: This is a huge topic that we could spend days talking about.

- **Asymmetric Warfare**
- **Passive Reconnaissance**
- **Automated Collection of Data**
- **Recon at scale**
- **First Contact**
- **Implications**
- **Recommendations**

Asymmetric Warfare

Background Discussion

1 SQL-Injection vs. 20 million lines of defensive code

$100 Dollar computer vs. $100 Million in defenses

1 economic DDoS script vs. $1 Million in wasted expenses

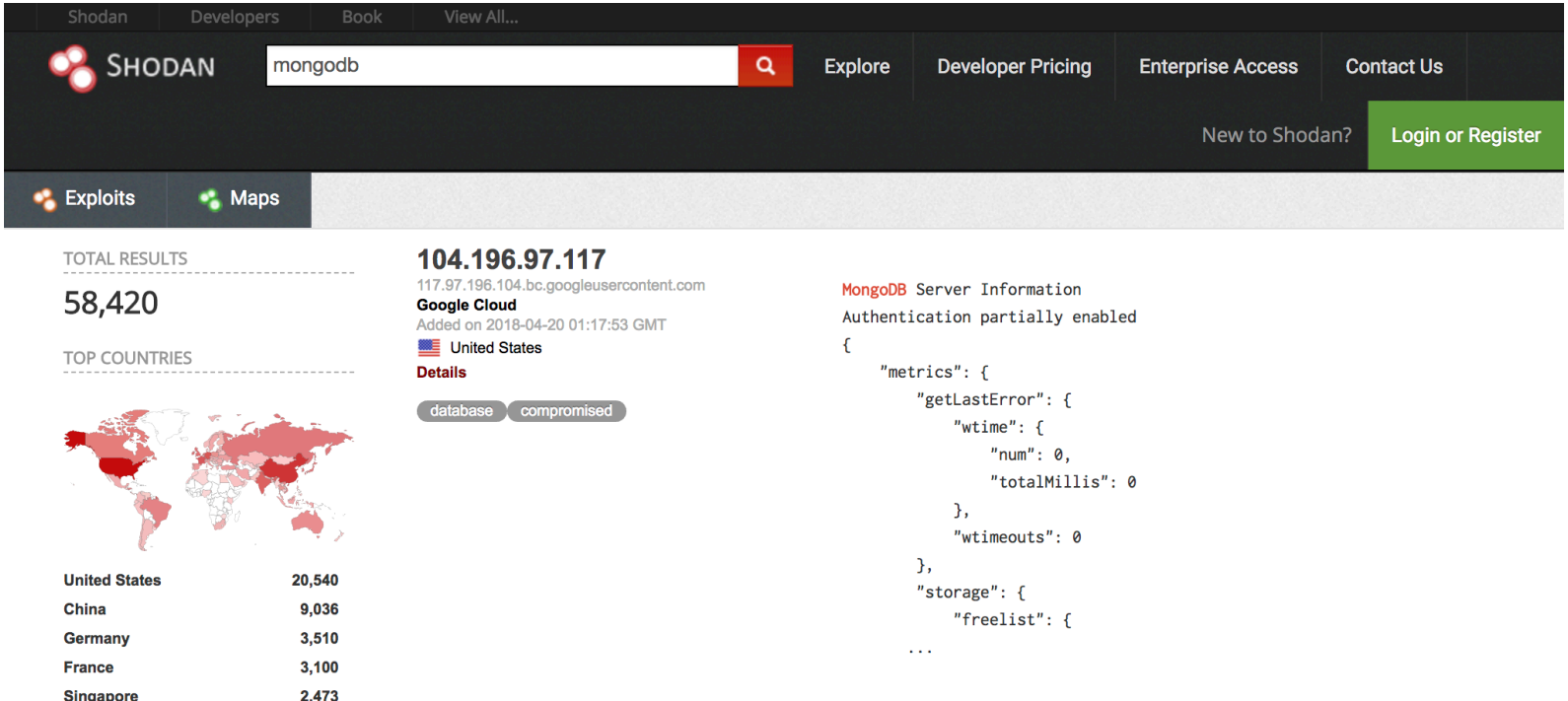
1:1,000,000+
Match vs. house

Note: This is a huge topic that we could spend days talking about.

- **Asymmetric Warfare**
- **Passive Reconnaissance**
- **Automated Collection of Data**
- **Recon at scale**
- **First Contact**
- **Implications**
- **Recommendations**

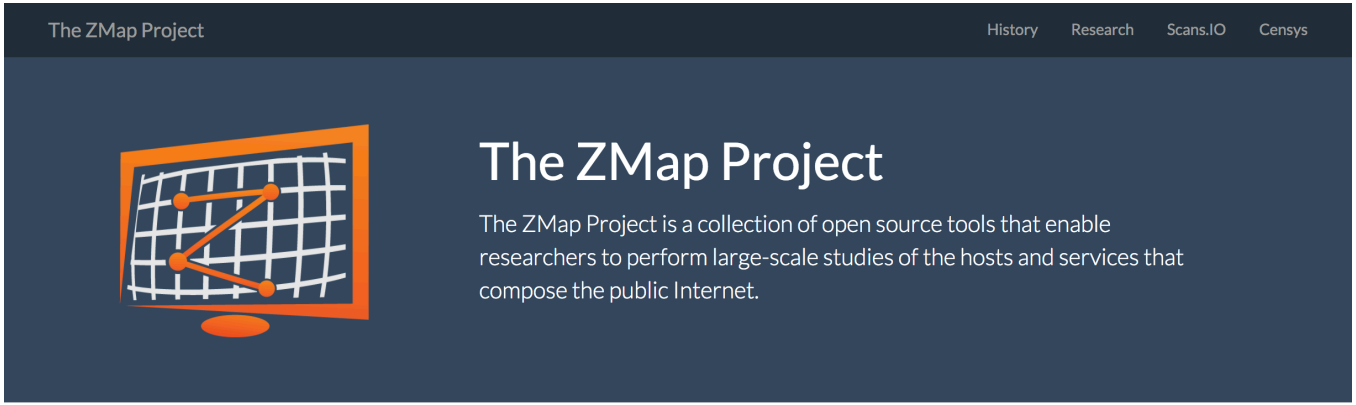
Shodan.io

Older method of getting global data



ZMAP.IO

Scan every IPv4 address in 5 Minutes



ZMap

ZMap is a fast single packet network scanner designed for Internet-wide network surveys. On a computer with a gigabit connection, ZMap can scan the entire public IPv4 address space in under 45 minutes. With a 10gigE connection and PF_RING, ZMap can scan the IPv4 address space in 5 minutes.

ZGrab

ZGrab is a stateful application-layer scanner that works with ZMap. ZGrab is written in Go and supports HTTP, HTTPS, SSH, Telnet, FTP, SMTP, POP3, IMAP, Modbus, BACNET, Siemens S7, and Tridium Fox. For example, ZGrab can perform a TLS connection and collect the root HTTP page of all hosts ZMap finds on TCP/443.

ZDNS

ZDNS is a utility for performing fast DNS lookups, such as completing an A lookup for all names in a zone file, or collecting CAA records for a large number of websites. ZDNS contains its own recursive resolver and supports A, AAAA, ANY, AXFR, CAA, CNAME, DMARC, MX, NS, PTR, TXT, SOA, and SPF records.

Masscan

https://github.com/robertdavidgraham/masscan

MASSCAN: Mass IP port scanner

This is the fastest Internet port scanner. It can scan the entire Internet in under 6 minutes, transmitting 10 million packets per second.

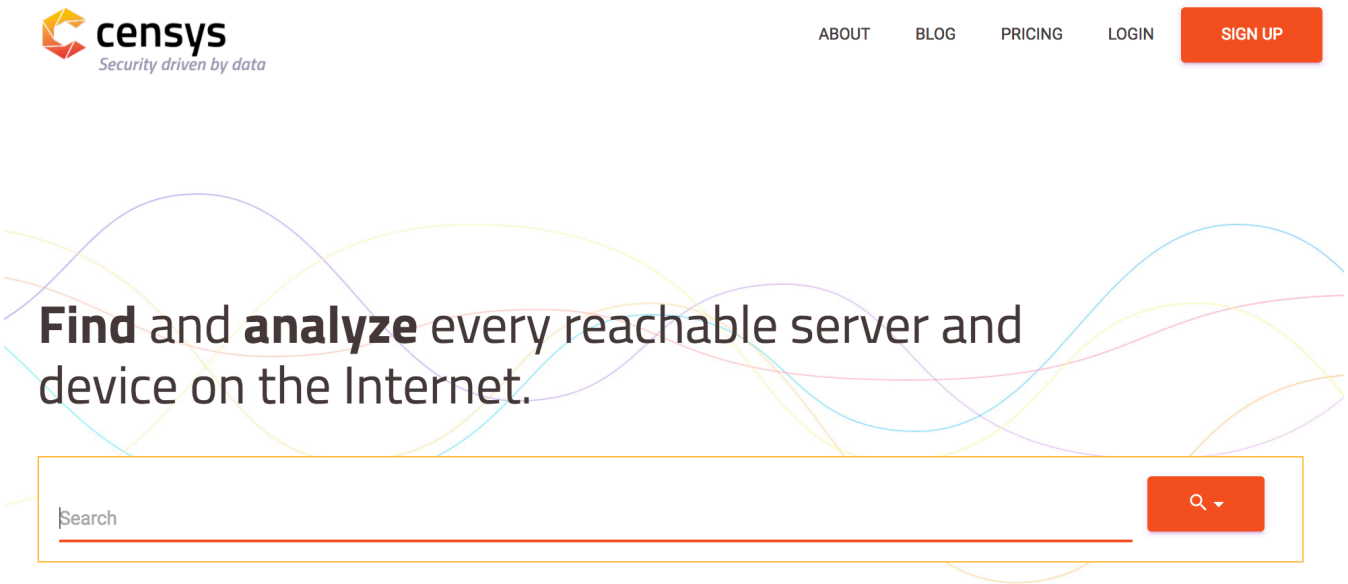
It produces results similar to `nmap`, the most famous port scanner. Internally, it operates more like `scanrand`, `unicornscan`, and `ZMap`, using asynchronous transmission. The major difference is that it's faster than these other scanners. In addition, it's more flexible, allowing arbitrary address ranges and port ranges.

NOTE: masscan uses a **custom TCP/IP stack**. Anything other than simple port scans will cause conflict with the local TCP/IP stack. This means you need to either use the `-S` option to use a separate IP address, or configure your operating system to firewall the ports that masscan uses.

This tool is free, but consider funding it here: 1MASSCANaHUiyTtR3bJ2sLGuMw5kDBaj4T

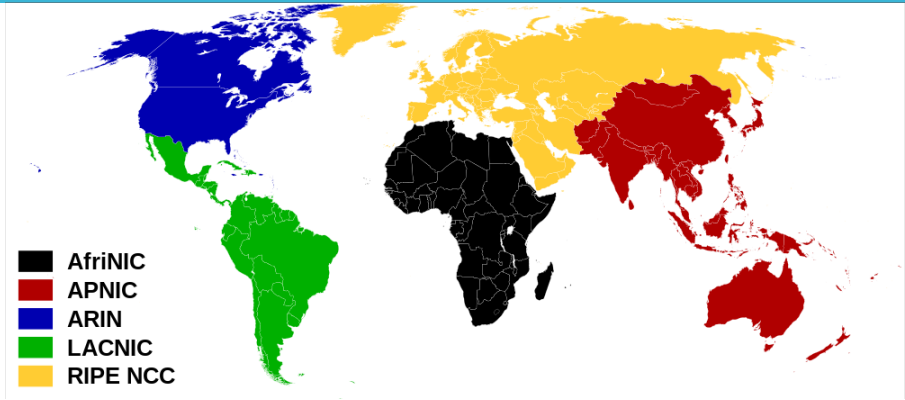
CENSYS

Many other public & private research groups like this.



Discussion

Finding IP Ranges



Search the 5 Regional Internet Registries for BGP Autonomous System Number Information

Finding IP Ranges

HURRICANE ELECTRIC INTERNET SERVICES

Randomly Chosen Seattle Based Company

Note: This will not Find all IP's

This is public data.

Search Results

Result	Description
AS22317	F5 Networks, Inc.
2620:0:c15::/48	F5 Networks, Inc.
2620:0:c14::/48	F5 Networks, Inc.
2620:0:c13::/48	F5 Networks, Inc.
2620:0:c12::/48	F5 Networks, Inc.
208.85.210.0/23	F5 Networks, Inc.
208.85.208.0/23	F5 Networks, Inc.
208.85.208.0/22	F5 Networks, Inc.
104.219.111.0/24	F5 Networks, Inc.
104.219.110.0/24	F5 Networks, Inc.
104.219.108.0/24	F5 Networks, Inc.
104.219.107.0/24	F5 Networks, Inc.
104.219.106.0/24	F5 Networks, Inc.
104.219.105.0/24	F5 Networks, Inc.
104.219.104.0/24	F5 Networks, Inc.

Finding IP Addresses

AS22317

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR

Country of Origin: United States

Prefixes Originated (all): 17
Prefixes Originated (v4): 13
Prefixes Originated (v6): 4

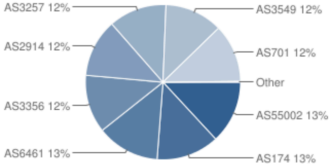
Prefixes Announced (all): 17
Prefixes Announced (v4): 13
Prefixes Announced (v6): 4

BGP Peers Observed (all): 11
BGP Peers Observed (v4): 11
BGP Peers Observed (v6): 4

IPs Originated (v4): 3,584
AS Paths Observed (v4): 2,404
AS Paths Observed (v6): 1,063

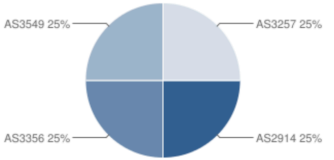
Average AS Path Length (all): 4.237
Average AS Path Length (v4): 4.259
Average AS Path Length (v6): 4.187

AS22317 IPv4 Peers



ASN	Name
AS55002	Defense.Net, Inc
AS174	Cogent Communications
AS6461	Zayo Bandwidth
AS3356	Level 3 Parent, LLC
AS2914	NTT America, Inc.
AS3257	GTT Communications Inc.
AS3549	Level 3 Communications, Inc. (GBLX)
AS701	Verizon Business/UUnet

AS22317 IPv6 Peers

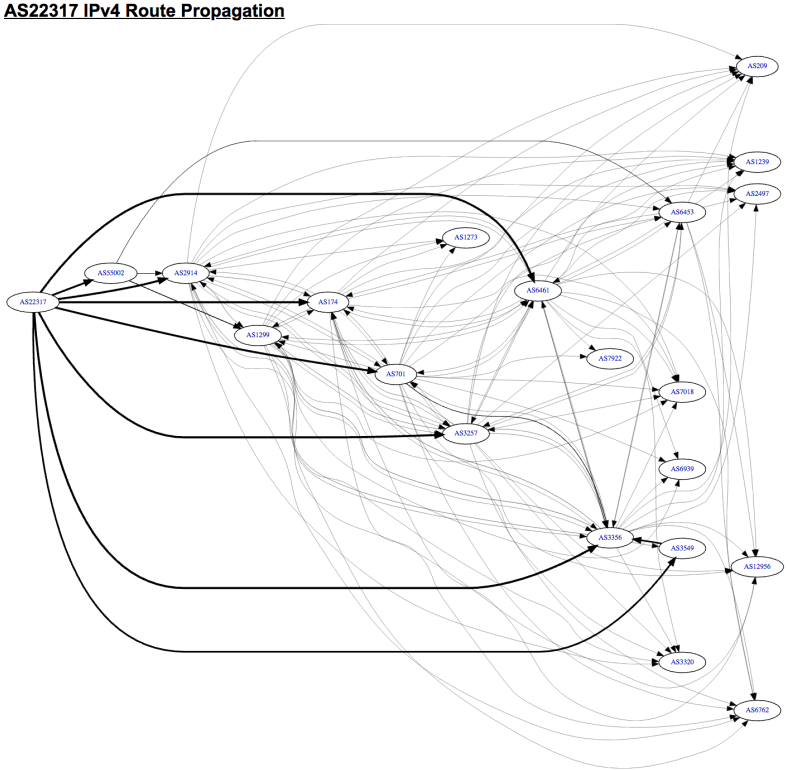


ASN	Name
AS2914	NTT America, Inc.
AS3356	Level 3 Parent, LLC
AS3549	Level 3 Communications, Inc. (GBLX)
AS3257	GTT Communications Inc.

Finding IP Addresses

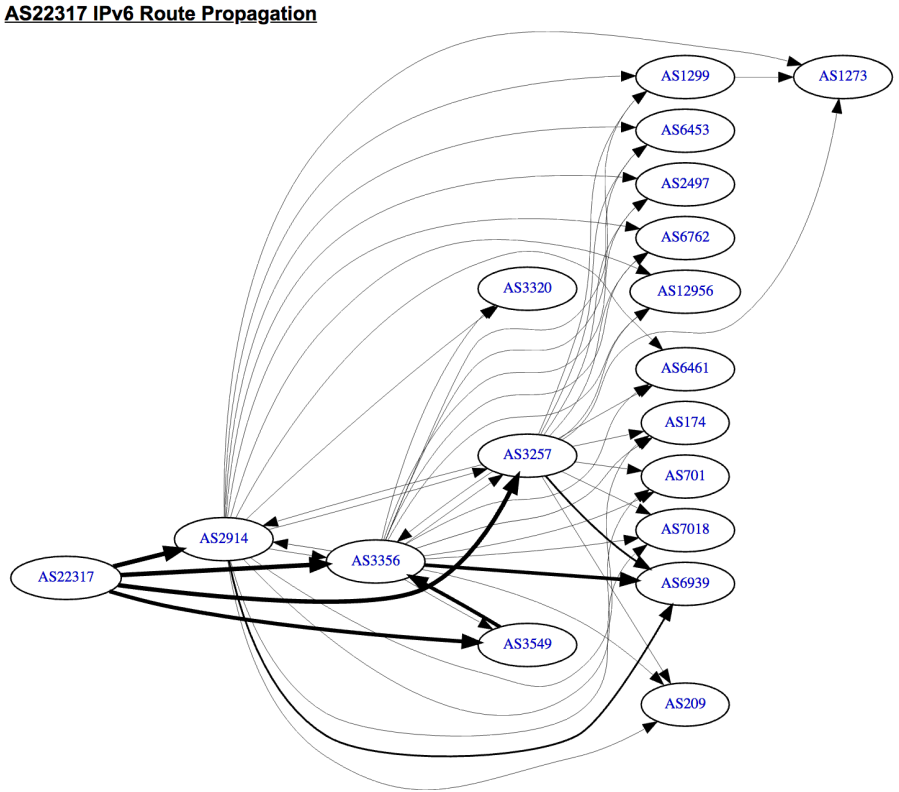
IPv4 Paths for AS22317

Automatically generated diagram to show routing paths



Finding IP Addresses

IPv6 Paths for AS22317



Finding IP Addresses

Address Ranges for AS22317

IPv4

Prefix	Description
65.197.145.0/24	MCI Communications Services, Inc. d/b/a Verizon Business
104.219.104.0/24	F5 Networks, Inc.
104.219.105.0/24	F5 Networks, Inc.
104.219.106.0/24	F5 Networks, Inc.
104.219.107.0/24	F5 Networks, Inc.
104.219.108.0/24	F5 Networks, Inc.
104.219.110.0/24	F5 Networks, Inc.
104.219.111.0/24	F5 Networks, Inc.
205.229.151.0/24	MCI Communications Services, Inc. d/b/a Verizon Business
208.85.208.0/22	F5 Networks, Inc.
208.85.208.0/23	F5 Networks, Inc.
208.85.210.0/23	F5 Networks, Inc.
209.194.169.0/24	Xspedius Communications Co.

IPv6

Prefix	Description
2620:0:c12::/48	F5 Networks, Inc.
2620:0:c13::/48	F5 Networks, Inc.
2620:0:c14::/48	F5 Networks, Inc.
2620:0:c15::/48	F5 Networks, Inc.

Note: This is a huge topic that we could spend days talking about.

SSL / TLS Certificate Discussion

Whois records for historical ownership matches, Secretary of State, GEOIP, OSINT, etc…

Many other steps, you get the idea.

Mapping DNS

Discussion

sales.company.com	200.1.1.1
dns1.company.com	200.1.1.2
dns2.company.com	200.1.1.3
mail1.company.com	200.1.1.4
mail2.company.com	200.1.1.5
www.company.com	is a CNAME, redirects to x4j5v.x.incapdns.net
barnyard.company.com	is a CNAME, redirects to x4j7a.x.incapdns.net

barnyard

Hint: incapdns is security related

Mapping Security

We can map most of their external security controls remotely without sending a single packet in.

We can even see things like:

- External Patching Frequency
- Internal Patching Frequency (user agents, version info)
- Cipher Strengths on all services
- Presence or absence of WAF's
- Honeypots in many cases, especially with historical information
- Firewall Rules including Egress rules in some cases
- Much more…

Mapping DNS

Quick point to watch out for:

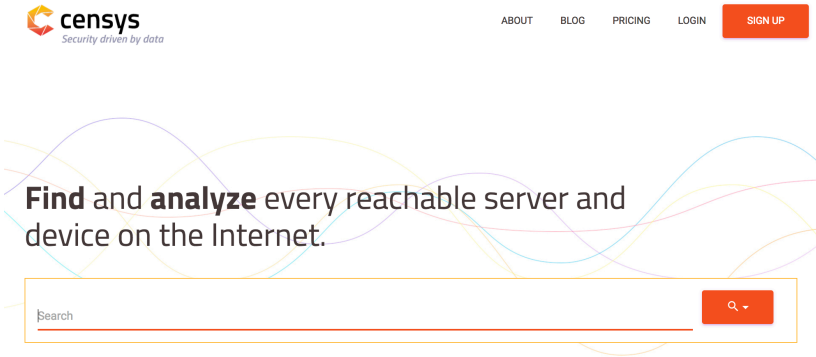
YOUR-COMPANY-NAME.VENDOR.COM

What could possibly go wrong ?

Your vendor agreements need to explicitly prohibit this.

Public Services

I can also gather what common TCP/IP services are listening for every IPv4 address and grab header version strings from 3rd party services or ZMAP type data.

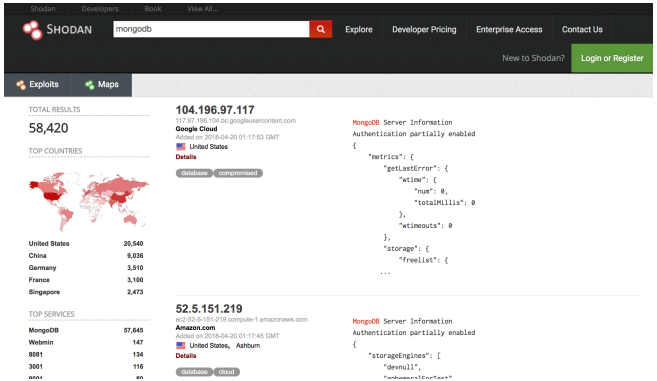


We can spot vulnerable services with this.

Open Ports via Shodan.io

NMAP NSE Plugin to scan ports via Shodan API

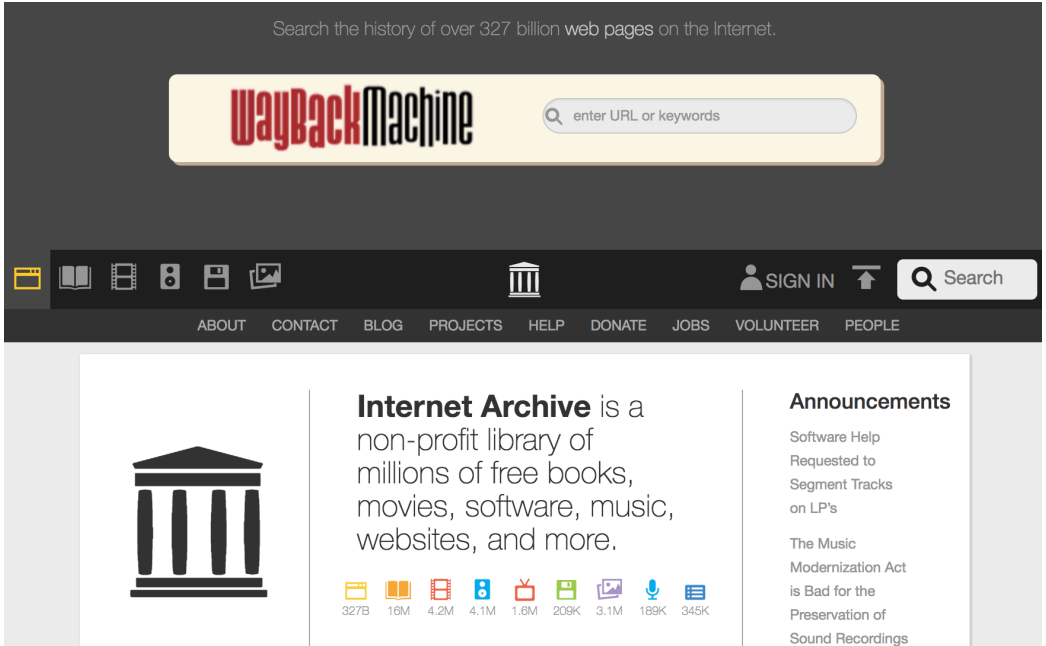
https://nmap.org/nsedoc/scripts/shodan-api.html



nmap --script shodan-api --script-args 'shodan-api.target=x.y.z.a,shodan-api.apikey=SHODANAPIKEY'

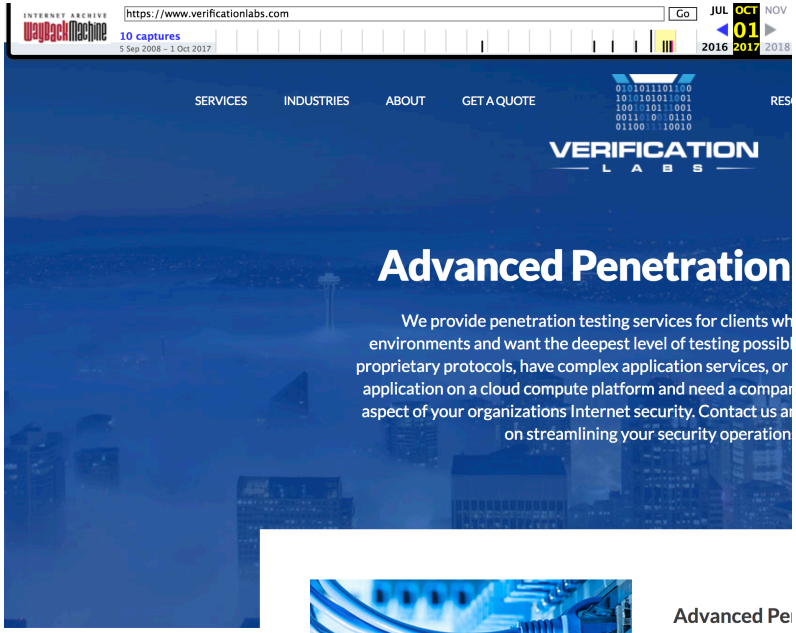
Wayback Machine

Discussion



Wayback Machine

Grab code from a 3rd party




```
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires
jQuery");+function(a){"use strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<
<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>2)throw new Error("Bootstrap's JavaScript requires
version 1.9.1 or higher, but lower than version 3")}(jQuery),+function(a){"use strict"
{var a=document.createElement("bootstrap"),b=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTr
otransitionend",transition:"transitionend"};for(var c in b)if(void
0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var
c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function()
{c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function()
{a.support.transition=b(),a.support.transition&&(a.event.special.bsTransitionEnd=
{bindType:a.support.transition.end,delegateType:a.support.transition.end,handle:functi
a(b.target).is(this)?b.handleObj.handler.apply(this,arguments):void 0})})}(jQuery),+f
{"use strict";function b(b){return this.each(function(){var
c=a(this),e=c.data("bs.alert");e||c.data("bs.alert",e=new d(this)),"string"==typeof
b&&e[b].call(c)})}var c='[data-dismiss="alert"]',d=function(b)
{a(b).on("click",c,this.close)};d.VERSION="3.3.6",d.TRANSITION_DURATION=150,d.prototyp
ion(b){function c(){g.detach().trigger("closed.bs.alert").remove()}var e=a(this),f=e.a
target");f||(f=e.attr("href"),f=f&&f.replace(/.*(?=#[^\s]*$)/,""));var
g=a(f);b&&b.preventDefault(),g.length||
(g=e.closest(".alert")),g.trigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented()||
(g.removeClass("in"),a.support.transition&&g.hasClass("fade")?
g.one("bsTransitionEnd",c).emulateTransitionEnd(d.TRANSITION_DURATION):c())};var
e=a.fn.alert;a.fn.alert=b,a.fn.alert.Constructor=d,a.fn.alert.noConflict=function(){re
a.fn.alert=e,this},a(document).on("click.bs.alert.data-api",c,d.prototype.close)}
(jQuery),+function(a){"use strict";function b(b){return this.each(function(){var
d=a(this),e=d.data("bs.button"),f="object"==typeof b&&b;e||d.data("bs.button",e=new
c(this,f)),"toggle"==b?e.toggle():b&&e.setState(b)})}var c=function(b,d)
{this.$element=a(b),this.options=a.extend({},c.DEFAULTS,d),this.isLoading=!1};c.VERSIO
EFAULTS={loadingText:"loading..."},c.prototype.setState=function(b){var
c="disabled",d=this.$element,e=d.is("input")?"val":"html",f=d.data();b+="Text",null==f
.data("resetText",d[e]()),setTimeout(a.proxy(function(){d[e](null==f[b]?
this.options[b]:f[b]),"loadingText"==b?(this.isLoading=!0,d.addClass(c).attr(c,c)):thi
(this.isLoading=!1,d.removeClass(c).removeAttr(c))},this),0)},c.prototype.toggle=funct
a=!0,b=this.$element.closest('[data-toggle="buttons"]');if(b.length){var
c=this.$element.find("input");"radio"==c.prop("type")?(c.prop("checked")&&
(a=!1),b.find(".active").removeClass("active"),this.$element.addClass("active")):"chec
("type")&&(c.prop("checked")!==this.$element.hasClass("active")&&
```

Wayback Machine

You can pull the functional website code including javascript files and scripts which access databases from the Wayback Machine.

Then search for vulnerabilities within that code.

Obviously we can scrape the site while posing as a search engine but we are operating in passive mode right now.

Wayback Machine

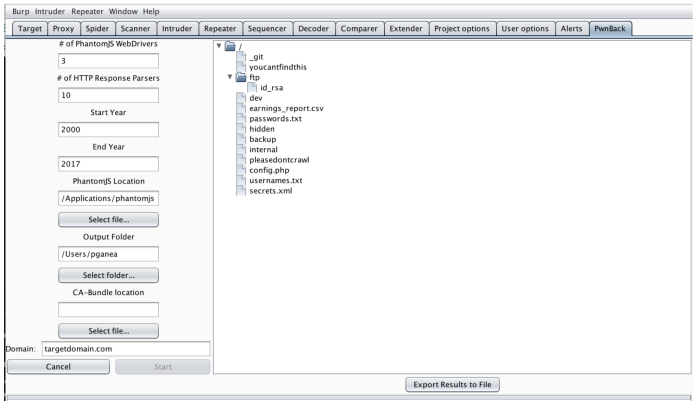
PwnBack is a BurpSuite plugin to effectively perform penetration tests against the copy of a website archived by the Wayback Machine

PORTSWIGGER
WEB SECURITY

Does this automatically for me and can be scripted.

BONUS: May find old code that still works and has vulns.

PwnBack



Other Data Sources

Password Dumps :: Key Dumps
Code Repositories like GitHub
Job postings
Former employee resumes
RFP’s
Twitter
Employees Social Media accounts
Google Alerts
Customer Forums
OSINT x 1000

Passive Recon

Important Point:

We still haven't sent a single packet to any of the targets systems.
(passive not active)

The attacker has an asymmetric advantage in that he or she knows a lot about the target but the target knows nothing about them yet.

Note: This is a huge topic that we could spend days talking about.

- **Asymmetric Warfare**
- **Passive Reconnaissance**
- **Automated Collection of Data**
- **Recon at scale**
- **First Contact**
- **Implications**
- **Recommendations**

Automated Collection of Data Discussion

Adversaries are playing a long game, yet most companies are just barely preparing to defend themselves against short games.

Their data about your network security may be better than your own.

Automation

Attackers only have to be lucky once, defenders have to be perfectly vigilant forever.*

Automation amplifies asymmetry

* = This has been said before, notably with different wording after an assassination attempt against Margaret Thatcher.

Automation

Automatic Exploitation Discussion

“Text me when you get a shell”

Note: This is a huge topic that we could spend days talking about.

- **Asymmetric Warfare**
- **Passive Reconnaissance**
- **Automated Collection of Data**
- **Recon at scale**
- **First Contact**
- **Implications**
- **Recommendations**

Recon at Scale (APT)

China										
Common Name	CrowdStrike	IRL	Kaspersky	Secureworks	Mandiant	FireEye	Symantec	iSight	Cisco (Sourcefire/\	Palo Alto U
Comment Crew	Comment Panda	PLA Unit 61398		TG-8223	APT 1			BrownFox	Group 3	
APT 2	Putter Panda	PLA Unit 61486		TG-6952	APT 2				Group 36	
UPS	Gothic Panda			TG-0110	APT 3		Buckeye	UPS Team	Group 6	
IXESHE	Numbered Panda			TG-2754 (tentative	APT 12	BeeBus		Calc Team	Group 22	
APT 16					APT 16					
Hidden Lynx	Aurora Panda				APT 17	Deputy Dog	Hidden Lynx	Tailgater Team	Group 8	
Wekby	Dynamite Panda	PLA Navy		TG-0416	APT 18					
Axiom					APT 17			Tailgater Team	Group 72	
Winnti Group	Wicked Panda									
Shell Crew	Deep Panda		WebMasters		APT 19	KungFu Kittens			Group 13	
Naikon	Lotus Panda	PLA Unit 78020	Naikon		APT 30					
PLATINUM										
Lotus Blossom			Spring Dragon							Lotus Blos
APT 6					APT 6					
Hurricane Panda	Hurricane Panda						Black Vine	TEMP.Avengers		
Emissary Panda	Emissary Panda			BRONZE UNION, T(	APT 27			TEMP.Hippo	Group 35	
Stone Panda	Stone Panda				APT 10			MenuPass Team		menuPass
Nightshade Panda	Nightshade Panda				APT 9					
APT 26					APT 26			Hippo Team		
Goblin Panda	Goblin Panda		Cycldek							
Night Dragon	Night Dragon									
Mirage	Vixen Panda	Ke3Chang		GREF	APT 15	Playful Dragon		Social Network Team		
Anchor Panda	Anchor Panda									
NetTraveler			NetTraveler		APT 21					
Ice Fog	Dagger Panda		IceFog							
Beijing Group	Sneaky Panda									
APT 22										

README | China | Russia | North Korea | Iran | Israel | NATO | Middle East | Others | Unknown | _Download | _Schemes | _Malware

Credit: @cyb3rops

Recon at Scale Discussion

APT's are focusing on entire industries for a reason. They are easier to map when you track them all and they Frequently share the same supply-chain insecurities.

Reminder: The data I've discussed thus far for an individual organization will easily fit on one hard-drive. Don't assume this is expensive to do.

Note: This is a huge topic that we could spend days talking about.

- **Asymmetric Warfare**
- **Passive Reconnaissance**
- **Automated Collection of Data**
- **Recon at scale**
- **First Contact**
- **Implications**
- **Recommendations**

First Contact

First contact used to be recon, now it's either a punch in the face or completely invisible.

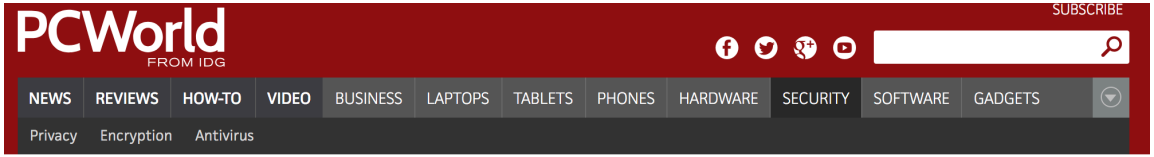
Think "working SQL-Injection attack pulling tables" as the first TCP packets coming in.

No time for humans to respond.

Weaponized bots scan the entire IPv4 space all the time.

MongoDB deletions

Example of scanning IPv4 IP's with an attack
Victims had no time to respond



Home / Security

NEWS

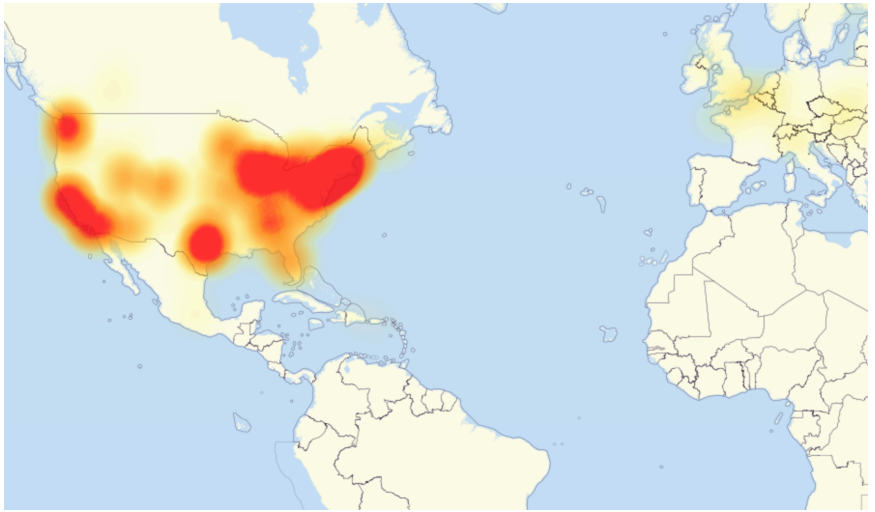
More than 10,000 exposed MongoDB databases deleted by ransomware groups

Five groups of attackers are competing to delete as many publicly accessible MongoDB databases as possible

By Lucian Constantin

Romania Correspondent, IDG News Service | JAN 6, 2017 9:35 AM PT

Dyn Cyberattack of 2016



Low-tech but very powerful and well-executed botnet attack consisting of tons of IoT devices with default passwords enabled.

Note: This is a huge topic that we could spend days talking about.

- **Asymmetric Warfare**
- **Passive Reconnaissance**
- **Automated Collection of Data**
- **Recon at scale**
- **First Contact**
- **Implications**
- **Recommendations**

Implications

Some traditional security processes aren't fast enough to respond or are simply no-longer relevant to modern attackers.

Attackers have automated their attacks
but many defenders still haven't automated their defenses.

Attacker asymmetry is growing.

Implications

Fake Security vs. Real Security

Short-term vs. Long-term thinking

Companies are diverging into two main camps.

Implications

The types of penetration testing and security assessments most companies are getting isn't sufficient and in many cases this reinforces the fake security models even to the companies that wanted real data and are striving to protect themselves.

Compliance in many ways creates and enables the "check box" fake security mentality. It's a necessary evil in ways but it's toxic to the companies wanting to do the right thing.

Implications

Security assessments should strive to be accurate and detailed like an MRI.

More importantly they should have a multitude of real-world solutions to problems found.

Some current product offerings in this area are very weak.

Implications

Important take away: **The gap between traditional security defenses and their effectiveness against automated offenses is widening quickly.**

Note: This is a huge topic that we could spend days talking about.

- **Asymmetric Warfare**
- **Passive Reconnaissance**
- **Automated Collection of Data**
- **Recon at scale**
- **First Contact**
- **Implications**
- **Recommendations**

MODUSBOX

Discussion on Recommendations

MODUSBOX

Questions

Trey.Blalock@Modusbox.com