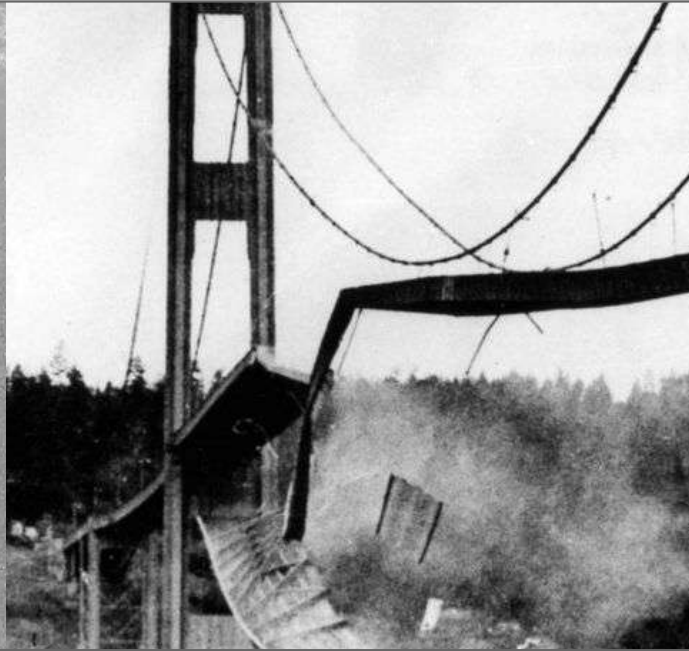


A LANDSCAPE OF UNINTENDED CONSEQUENCES



Sarah Allen
@ultrasaurus



Location: about

[What's New!](#) [What's Cool!](#) [Handbook](#) [Net Search](#) [Net Directory](#) [Software](#)


NETSCAPE

Netscape Navigator ^(TM)

Version 2.02

Copyright © 1994-1995 Netscape Communications Corporation. All rights reserved.

This software is subject to the license agreement set forth in the [license](#). Please read and agree to all terms before using this software.

Report any problems through the [feedback page](#).

Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape Communications Corporation.



JAVA COMPATIBLE

Contains JavaTM software developed by Sun Microsystems, Inc.
Copyright © 1992-1995 Sun Microsystems, Inc. All Rights Reserved.



Contains security software from RSA Data Security, Inc.
Copyright © 1994 RSA Data Security, Inc. All rights reserved.

This version supports International security with RSA Public Key Cryptography, MD2, MD5, RC4.

Any provision of Netscape Software to the U.S. Government with "Restricted rights" as follows: Use, duplication or disclosure by the Government is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Restricted Rights clause at FAR 52.227-19 when applicable, or in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, and in similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Netscape Communications Corporation, 501 East Middlefield Road, Mountain View, California, 94043.

Perimeter Security

Motte and Bailey Castles



Director Commands Disabled for Shockwave

Although the good news is that additional Net-related commands were added for shocked movies, the bad news is that other Director commands have been disabled.

Although a variety of commands have been disabled, most of them relate to data transmission. The primary reasons for disabling commands are to prevent the transfer of viruses and to block the capability to read information off of a user's hard drive and transfer that information back through the shocked movie to a Web site. Lingo, like virtually all other programming languages, can read, write, and delete files. Therefore, if certain capabilities were not disabled, the shocked movies, via Lingo, would have access to users' hard drives, where they could extract information (upload local files, including both data and programs), delete information (delete local files and programs or entire drives), or introduce information (alter files, add files, add viruses).

The following commands have been disabled in Director 4.0x and Director 5 shocked movies.

Table 29.1 shows Director-related commands that open, close, paste, print, and save files.

Table 29.1. Disabled Director-related commands.

<i>Command</i>	<i>Description</i>
openResFile	This Mac-only command opens a specific resource file. Because shocked movies might be played in Windows or another operating system, this command has been disabled to prevent errors.
closeResFile	The counter command to the openResFile command closes a resource file that has been opened on a Mac. It has been disabled for the same reasons as the openResfile command.
open window	Director has the capability of playing a second movie inside of an opened Director movie. You can size this "windowed" movie from very small to large enough to occupy the entire screen size of the current movie. Because the Windows version of Shockwave currently has problems with Director windows, and because Netscape supports only Director windows if the EMBED command is used, this feature has been disabled. Macromedia is working to resolve this problem.
close window	This command closes an open Director window, but because opening Director windows has been disabled, this command is also disabled.
importFileInto	Castmembers (the objects-graphics, scripts, videos, and so on) that are used in a Director movie are all referred to as castmembers. Most often, all castmembers are saved inside of the Director movie. The importFileInto command enables an external file to be loaded into a castmember position of a Director movie, either replacing one of the movie's castmembers or adding a new castmember to the movie. As already mentioned, to maintain system integrity, all I/O or data transfer functions have been disabled; importFileInto falls into this category and has been

Netscape - [Plug-ins and HTML]

Datei Bearbeiten Anzeigen Gehe Les

Adresse: file:///e:/vp11/prog/wp32/npwin32.htm

Plug-ins and HTML

NPWin32 plug-in



Plugin above!

LEGO - BUILD - Microsoft Internet Explorer

Subito Úpravy Zobrazit Obľíbené Nástroje Návod ↵ Zpět ↵ ↵ Hledat Obľíbené Média ↵

Adresa: http://www.lego.com/build/games/

SHOP ONLINE | SERVICE | PRIVACY | Sign in

LEGO Portals Product Finder

Home > BUILD

Games & Activities

Junkbot
Junkbot needs your help! He's got to collect all the trash in a huge factory, and only you can build the stairs, bridges, and walls to get him around. (Requires Shockwave 8.)

Brick Builder
Ever wish you had an infinite bucket of LEGO bricks? With Brick Builder, you can create anything you can imagine, using dozens of different virtual bricks... and you'll never run out! (Requires Macromedia Flash.)



Checkout a [list of sites](#) using FutureSplash to enhance the user experience without slowing the user down. Don't miss the new [MSN](#) and [Simpsons](#) sites! Celebrate the [birthday of Sint Nicolaas](#) in Holland before December 6. Try the updated [Support](#) area.



FutureSplash Player 1.1 Available

The [1.1 version](#) of FutureSplash Player is now available. It adds support for Netscape LiveConnect and improved memory management on the Mac. Internet Explorer users got it automatically, Netscape users can [upgrade now](#). Once you get it, try our new [scripting demo](#).

FutureSplash Animator Is Shipping!

[FutureSplash Animator](#) is now available for Macintosh and Windows 95/NT. Order your copy today.

Microsoft Network (MSN) goes on-line with FutureSplash Animator!



+ "ActionScript"



+ RTMP (two way audio-video)

ORANGES

APPLES

BANANAS

CARROTS

LETTUCE

BEANS

CANS

APPLE SAUCE

BEAN SOUP

TOMATO SOUP

CEREALS

BREAD

NOODLES (ELBOW KIND)

FRENCH BREAD

COLD LOCKER

MILK



abc

sponsored by *Suave*



Lost

Desperate Housewives

Commander in Chief

Alias



Desperate Housewife 0:02 / 43:08



Episode: Special 220 221 **222** 223

The ABC logo is a white lowercase 'abc' inside a dark blue circle with a glowing white border. It is positioned in the upper left quadrant of the interface.The word 'ALIAS' is written in a white, sans-serif font, slanted upwards to the right. It is located in the top left panel of the carousel.The word 'LOST' is written in a white, bold, sans-serif font. It is located in the top right panel of the carousel.The word 'ALIAS' is written in a white, sans-serif font, slanted upwards to the right. It is located in the middle left panel of the carousel.The word 'LOST' is written in a white, bold, sans-serif font. It is located in the middle right panel of the carousel.The word 'ALIAS' is written in a white, sans-serif font, slanted upwards to the right. It is located in the bottom left panel of the carousel.The word 'LOST' is written in a white, bold, sans-serif font. It is located in the bottom middle panel of the carousel.

ABC.com Full Episode Streaming

Click on the show you'd like to watch. If it's not already in the center position, it'll rotate there. Once it's centered, click on the image again to focus on that show. To watch the episode, click the play button.

© 2009 ABC. All rights reserved. ABC and the ABC logo are trademarks of ABC. All other trademarks are the property of their respective owners.

Common Vulnerabilities and Exposures 2001-2019

1172

2001-2019 CVE reports

1172 Flash Player

1999 Internet Explorer

2033 Chrome

2442 Firefox

2001-2019 CVE reports

1172 Flash Player

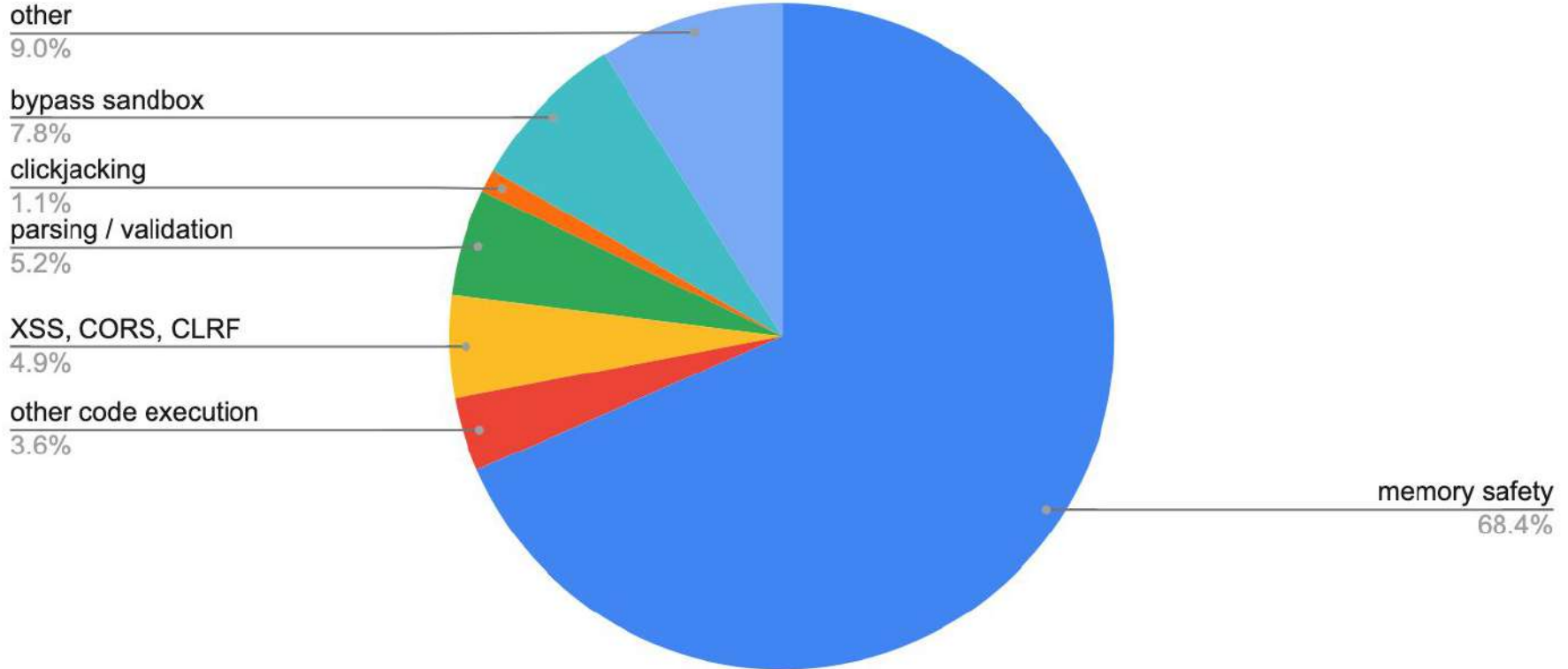
1999 Internet Explorer

2033 Chrome

2442 Firefox

number is ***not significant*** indicator

Flash Player CVEs



Memory Safety CVEs

337	memory corruption
262	use after free
116	buffer overflow
35	integer overflow
17	out-of-bounds read
9	heap.overflow
8	null pointer dereference
5	double free
4	bounds checking
3	out of bounds memory read
3	improper memory access
2	out-of-bounds write
1	invalid pointer dereference

Memory Safety CVEs

337 memory corruption

262 use after free

116 buffer overflow

35 integer overflow

17 out-of-bounds read

9 heap.overflow

8 null pointer dereference

5 double free

4 bounds checking

3 out of bounds memory read

3 improper memory access

2 out-of-bounds write

1 invalid pointer dereference

“allows remote attackers to execute arbitrary code via a crafted SWF file”

“allows remote attackers to execute arbitrary code via crafted streaming media”

“allows remote attackers to execute arbitrary code via a crafted font”


```
long a = (long)b;
```

Unexpected Context

...allows remote attackers to cause victims to unknowingly click on a link or dialog via access control dialogs disguised as normal graphical elements, as demonstrated by hijacking the camera or microphone

Microsoft Excel allows user-assisted attackers to execute arbitrary javascript and redirect users to arbitrary sites via an Excel spreadsheet with an embedded Shockwave Flash Player ActiveX Object, which is automatically executed when the user opens the spreadsheet.

...spooft the address bar and possibly conduct phishing attacks by re-opening the window to a malicious Shockwave Flash application, then changing the window location back to a trusted URL while the Flash application is still loading

Unexpected Context \Rightarrow Parsing / Validation

not properly validate

malformed header overflow

type confusion

object confusion

does not verify a member element's size

wide characters

untrusted input

xml script


interpret jar: URLs

CRLF injection

modify HTTP headers

Recent vulnerabilities in URL parsing...

route regex match fails for large URIs #7728

 Closed skambashi opened this issue on Jul 25 · 13 comments



skambashi commented on Jul 25 · edited ▾

Description:

We've noticed that requests with a very long URI crashes our envoy service for routes defined using a regex matcher.

We're not sure if it's due to some overflow bug in Envoy's regex parser, but ideally Envoy should not crash because of a long URI.

Repro steps:

Define a route with a match regex like the following:

```
"match": {
  "regex": "/asdf/.*"
}
```

and then make a request with a large URI:

```
val longString = "a" * (50 * 1024)
client.send("GET", "/asdf/{longString}")
```

We've gotten around it by using a `prefix` matcher instead, but this appears to be a potential DoS vulnerability if not a security issue.

<https://github.com/envoyproxy/envoy/issues/7728>

Recent vulnerabilities in URL parsing...

net/url: make Hostname and Port predictable for invalid Host values

When Host is not valid per RFC 3986, the behavior of Hostname and Port was wildly unpredictable, to the point that Host could have a suffix that didn't appear in neither Hostname nor Port.

This is a security issue when applications are applying checks to Host and expecting them to be meaningful for the contents of Hostname.

To reduce disruption, this change only aims to guarantee the following two security-relevant invariants.

- * Host is either Hostname or [Hostname] with Port empty, or Hostname:Port or [Hostname]:Port.

- * Port is only decimals.

The second invariant is the one that's most likely to cause disruption, but I believe it's important, as it's conceivable an application might do a suffix check on Host and expect it to be meaningful for the contents of Hostname (if the suffix is not a valid port).

<https://go-review.googlesource.com/c/go/+189258/>

Your implementation is your API.

Your implementation is your API.
(not your docs)

The dark ages

Web is for *content*

Physical networks

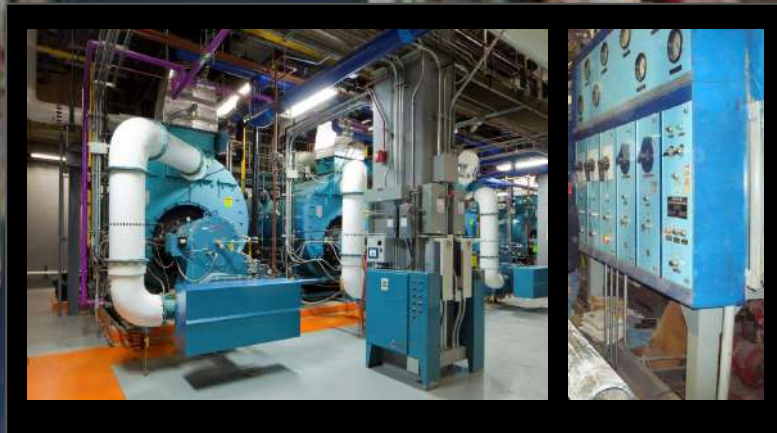
Perimeter security

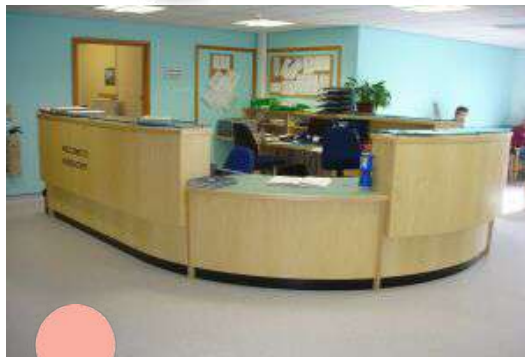
HTTPS is expensive

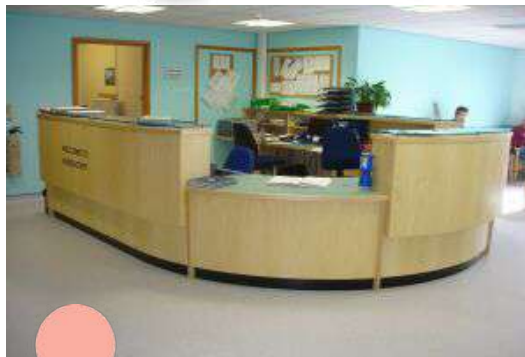


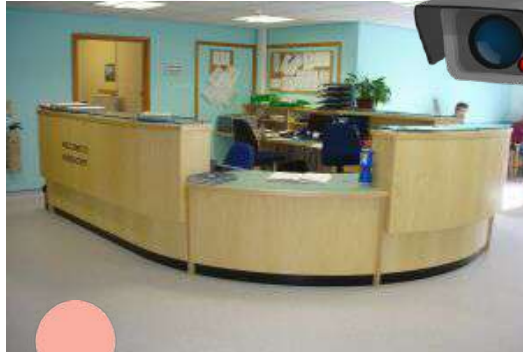


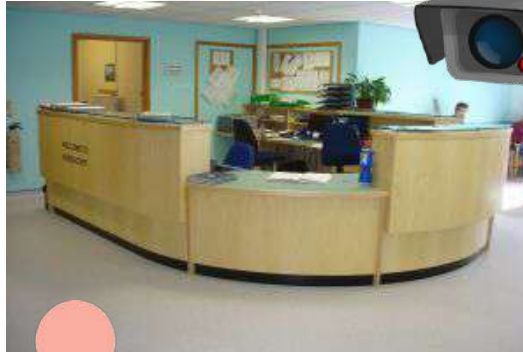












[PROVIDERS](#)[SPECIALTIES](#)[LOCATIONS](#)[HEALTH EDUCATION](#)[PATIENT RESOURCES](#)[OUR COMPANY](#)

Google™ Search

powered by Google™

[FIND A PROVIDER](#)[FIND A SPECIALTY](#)[HEALTH EDUCATION](#)*Exceptional Doctors*

Healthy You

[MANAGE YOUR HEALTH ONLINE](#)

GREAT AMERICAN SMOKEOUT



You Can Do It! We're Here to Help. Today is The Great American Smokeout. Click here to find out how we can help you or a loved one quit smoking today.

GIVE THE GIFT OF BEAUTY



A gift for a loved one or a present to yourself, take advantage of these holiday offers; Botox, Juvederm, Restylane and Radiesse 20% off. Click here to print off your coupon.

SIGN UP FOR E-NEWSLETTERS



Subscribe to our e-newsletter & receive... general health tips, special discounts and health & wellness class information.



Designing unique EHR interfaces for different hospitals, care settings, and specialties may improve EHR usability.



Source: Thinkstock

<https://ehrintelligence.com/news/will-specializing-ehr-interfaces-solve-the-ehr-usability-problem>

BUILDING ANALYTICS

Drive results to improve energy and operational efficiency, and tenant comfort



Buildings in the US that we're currently helping to achieve higher performance in terms of efficiency, with additional facilities added weekly
*Current as of January 2014

Building managers can access pre-designed daily diagnostic reports to pinpoint building system irregularities, avoidable costs, building comfort impacts and more. All reports are fully customizable too



Diagnostics are fully automated. Plus, our experts periodically validate system level root cause analysis to further prioritize cost-saving recommendations for you and your decision makers



Fewer comfort complaints recorded



Identification of avoidable HVAC energy costs, which results in a substantial increase in overall energy savings



Decrease in maintenance incidents according to our reports

Associated Points

- The Cloud
- Web hosted — minimal local infrastructure support
- Minimal install costs
- Incredibly Secure — we use Microsoft Azure™
- Seamless backup
- Internet access for remote connectivity

Pieces of equipment currently monitored by Schneider Electric

- Air handling units (AHU)
- Zone and terminal units — flow, temperature, humidity, valves
- Central plant pumps
- Towers
- Chillers
- Valves
- Boilers
- Whole building meters — gas, electric, water & more

Data points captured through Building Management Systems every five minutes



Data points per day that our Cloud analyzes and converts into actionable comfort, operational and energy performance opportunities



BENEFITS



Increase awareness of building performance and issues with prioritized recommendations



Validate HVAC retrofits and enhancements that uncover hidden savings



Ongoing commissioning and sustainability to achieve measurable return



Knowing the financial implications to manage building decisions and resources more efficiently



Actionable intelligence helps to effectively and proactively manage business operations



Schneider Electric



20.8
BILLION
connected things
by 2020¹



500+%
Growth in health
consumer IoT
connections from
2015-2020²



1.3
TRILLION
worldwide spending
on IoT by 2019³



680%
Growth of installed
base of healthcare
IoT devices by 2020⁴

The dark ages

Web is for *content*

Physical networks

Perimeter security

HTTPS is expensive

The modern era

PII + finance + real-world

Bot armies

Supply chain attacks

Cloud native

Ubiquitous crypto





Humans make errors.

The world is changing.



Home » Cyber Events » Cyber Attacks » Samsung Smart Refrigerator Hacked, Left Gmail Login Credentials Vulnerable

Samsung Smart Refrigerator Hacked, Left Gmail Login Credentials Vulnerable

info security Latest
STRATEGY | INSIGHT | TECHNOLOGY
Why the Security Industry Should Pay Attention to the Cisco Whistleblower Case

Home News Topics Features Webinars White Papers Podcasts Events & Conferences Directory

INFOSECURITY MAGAZINE HOME » NEWS » TARGET HACKERS MAY HAVE GOTTEN IN THROUGH THE AIR CONDITIONER

6 FEB 2014 **NEWS**
Target Hackers May Have Gotten In Through the Air Conditioner

Malicious Code Injection Strikes Again as npm Foils \$13M Cryptocurrency Theft

June 07, 2019 By Derek Weeks

Motherboard

How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet

As many predicted, hackers are starting to use your Internet of Things to launch cyberattacks.

By **Lorenzo Franceschi-Bicchieri**

Sep 29 2016, 9:03am [f Share](#) [t Tweet](#)

Fundamentals are the same.

Vulnerabilities
create
opportunity.

Target Settles HVAC Data Breach for \$18.5 Million

[Home](#) > [Security](#)

FEATURE

11 Steps Attackers Took to Crack Target

Aorato, a specialist in Active Directory monitoring and protection, delivers a step-by-step report on how attackers used the stolen credentials of an HVAC vendor to steal the data of 70 million customers and 40 million credit cards and debit cards from the retailer.

<https://www.cio.com/article/2600345/11-steps-attackers-took-to-crack-target.html>

8 vulnerabilities

1. Install malware that steals credentials
2. Exploit a web application vulnerability
3. Steal access token from domain admins
4. Run code to find computers on the network
5. SQL database \Rightarrow 70M PII
6. PoS, custom malware \Rightarrow *40M credit cards*
7. Create network share for stolen data
8. Exfiltrate data via FTP \Rightarrow success

The initial penetration point is not the story, because eventually *you have to assume you're going to get breached...* You cannot assume otherwise. You have to be prepared and have an incident response plan for what to do when you are breached. The real problem arises when malware is able to enable an attacker to penetrate deeper into the network."

— Tal Be'ery, Aorato Lead Researcher

Plot to steal cryptocurrency foiled by npm security

Popular pattern

1. publish a “useful” package
2. waiting until in use by the target,
3. update to include malicious code..

It now seems clear that the bug was created intentionally to target Komodo's version of Agama wallet. **A hacker spent several months making useful contributions...before inserting the bug.** Eventually, the hacker added malicious code to an update of a module that Komodo's Agama was already using.

– komodoplatform.com/update-agama-vulnerability

What's new today?

What's new today?

Scale

Everything is connected

Real-world targets

Lessons learned

Lessons learned

Secure is a verb, not an adjective.

Lessons learned

Secure is a verb, not an adjective.

Anything that can happen, will.

Lessons learned

Secure is a verb, not an adjective.

Anything that can happen, will.

Don't create new parser or new crypto,
unless you need to.

Lessons learned

Secure is a verb, not an adjective.

Anything that can happen, will.

Don't create new parser or new crypto, unless you need to. Invent ***new*** things!

Lessons learned (practical tips)

Tools for testing, monitoring.

Lessons learned (practical tips)

Tools for testing, monitoring.

Memory safe languages / features

Lessons learned (practical tips)

Tools for testing, monitoring.

Memory safe languages / features

Contribute to open source dependencies

Checklists are an anti-pattern.

Checklists are an anti-pattern.



github.com/cncf/sig-security

Checklists are an anti-pattern.



github.com/cncf/sig-security



before-you-ship.18f.gov/security



bestpractices.coreinfrastructure.org

@ultrasaurus