Increased Telework and Security Implications

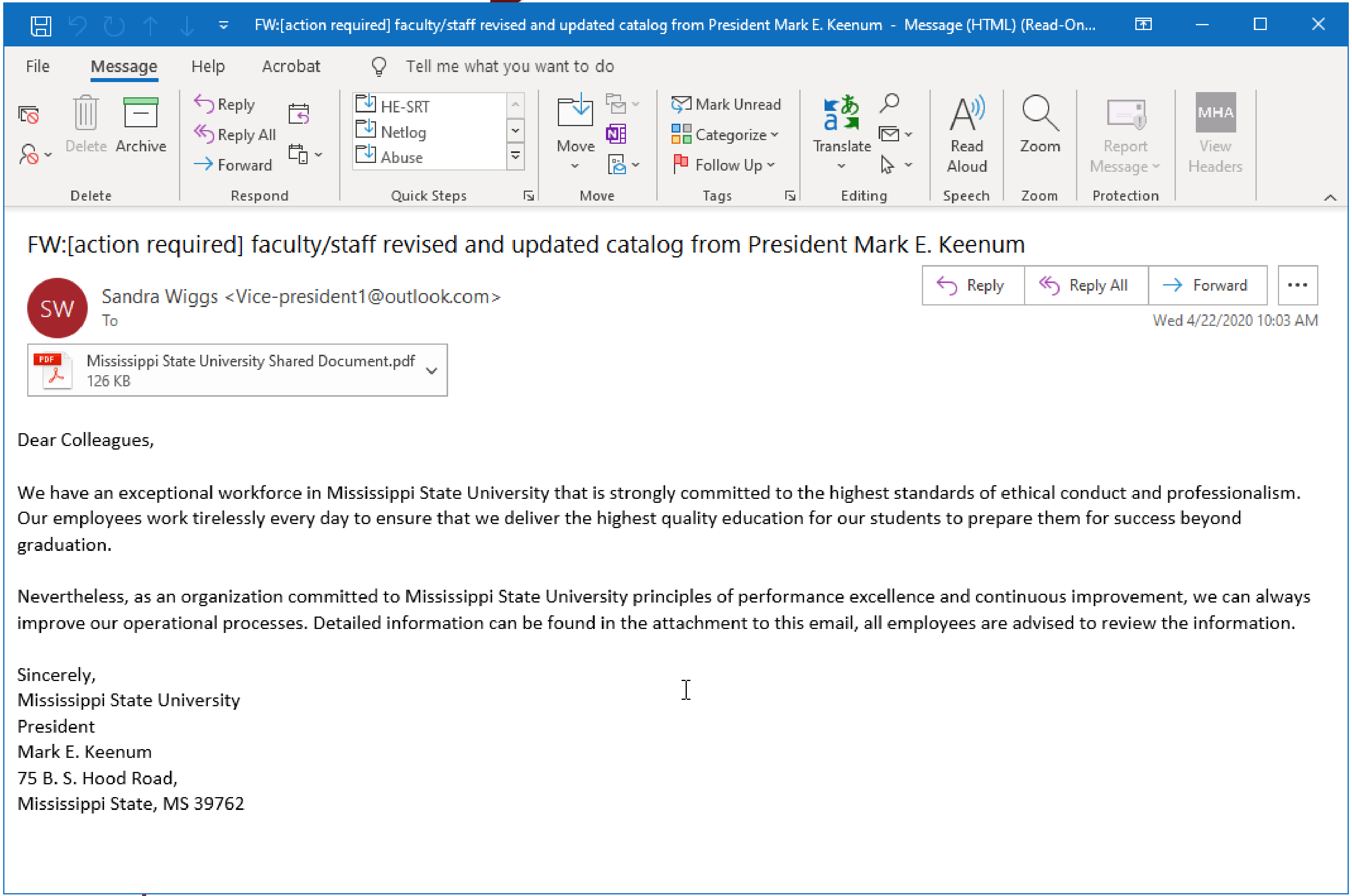
Tom Ritter
Security and Compliance Officer
Office of the CIO

MISSISSIPPI STATE UNIVERSITY
INFORMATION TECHNOLOGY SERVICES

Protecting campus in this time of telework – Why is Email Central?

- Email is the most common attack vector
- *91% of targeted attacks start with email – Proofpoint*
- ~10% of MSU users WILL answer a phish – 2017 penetration testing statistic
- Email compromise attacks more common than ever. IE. "Are you available?" Gift cards scams, sextortion, job offers, fake HRM notices, etc.

Targeted Phish



FW:[action required] faculty/staff revised and updated catalog from President Mark E. Keenum

Sandra Wiggs <Vice-president1@outlook.com>
To

Wed 4/22/2020 10:03 AM

Mississippi State University Shared Document.pdf
126 KB

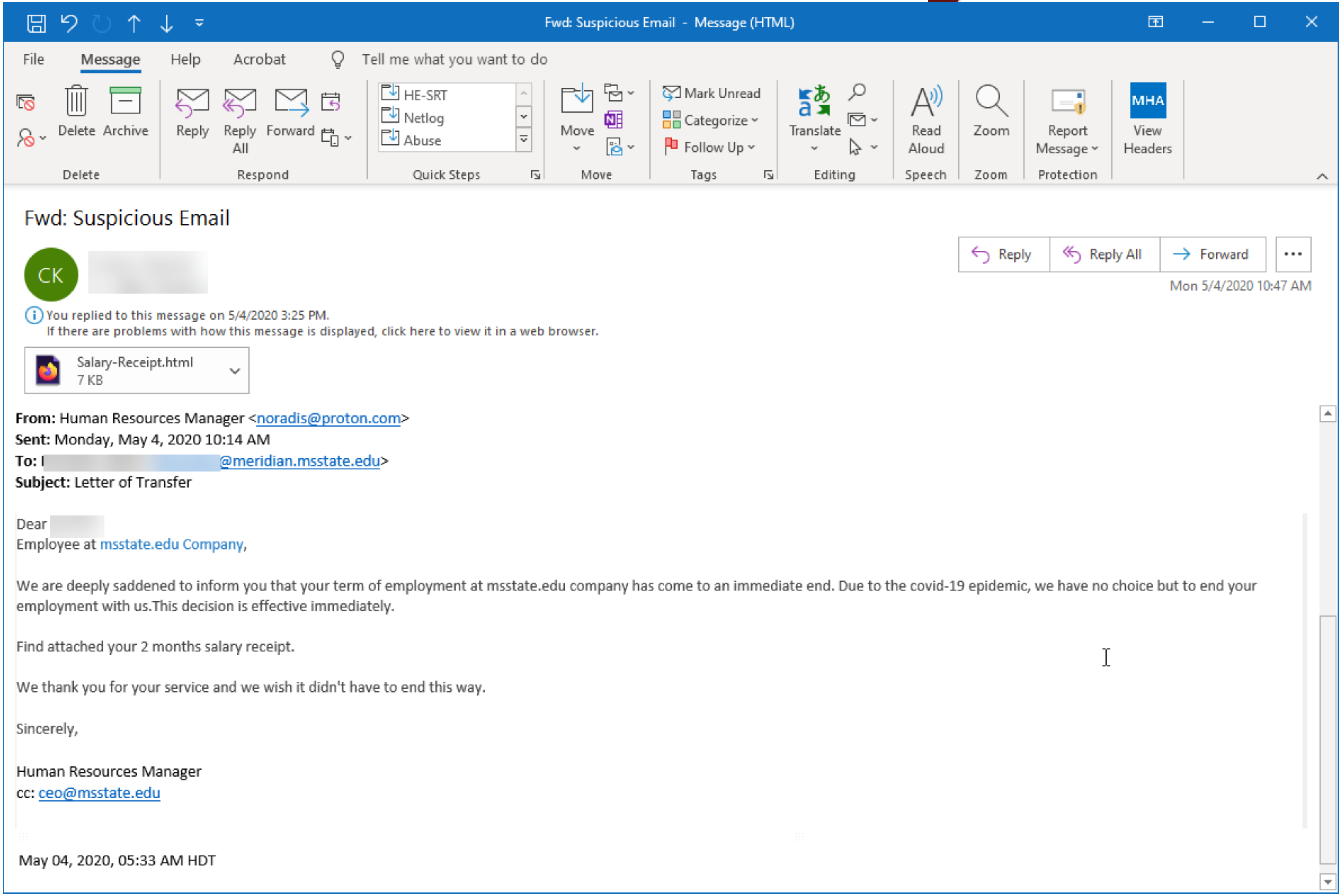
Dear Colleagues,

We have an exceptional workforce in Mississippi State University that is strongly committed to the highest standards of ethical conduct and professionalism. Our employees work tirelessly every day to ensure that we deliver the highest quality education for our students to prepare them for success beyond graduation.

Nevertheless, as an organization committed to Mississippi State University principles of performance excellence and continuous improvement, we can always improve our operational processes. Detailed information can be found in the attachment to this email, all employees are advised to review the information.

Sincerely,
Mississippi State University
President
Mark E. Keenum
75 B. S. Hood Road,
Mississippi State, MS 39762

Covid-19 Phishing



Fwd: Suspicious Email

[redacted]

Mon 5/4/2020 10:47 AM

You replied to this message on 5/4/2020 3:25 PM.
If there are problems with how this message is displayed, click here to view it in a web browser.

Salary-Receipt.html
7 KB

From: Human Resources Manager <noradis@proton.com>
Sent: Monday, May 4, 2020 10:14 AM
To: [redacted]@meridian.msstate.edu>
Subject: Letter of Transfer

Dear [redacted]
Employee at msstate.edu Company,

We are deeply saddened to inform you that your term of employment at msstate.edu company has come to an immediate end. Due to the covid-19 epidemic, we have no choice but to end your employment with us.This decision is effective immediately.

Find attached your 2 months salary receipt.

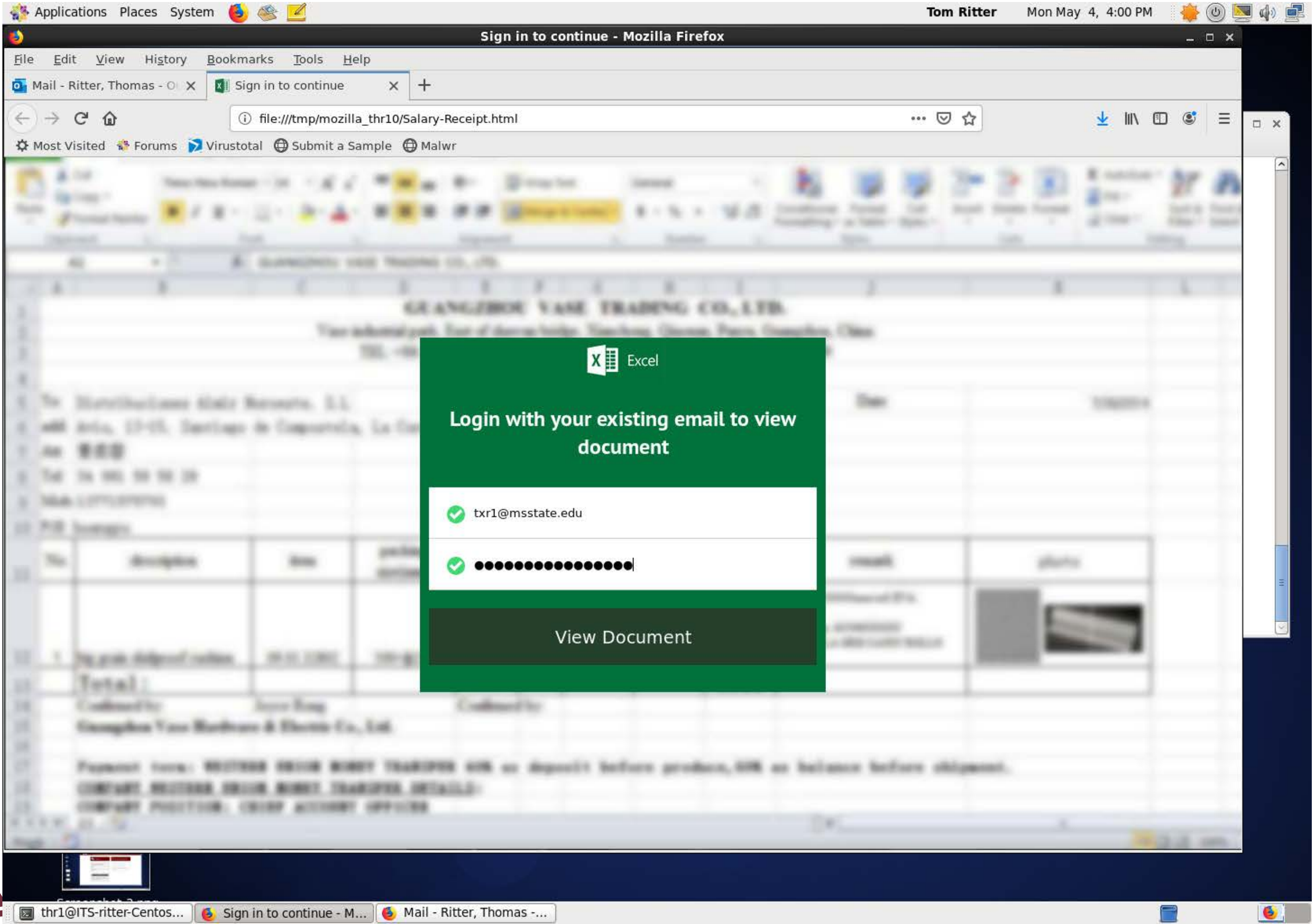
We thank you for your service and we wish it didn't have to end this way.

Sincerely,

Human Resources Manager
cc: ceo@msstate.edu

May 04, 2020, 05:33 AM HDT

Covid-19 Phishing


Applications Places System
Tom Ritter Mon May 4, 4:00 PM
File Edit View History Bookmarks Tools Help
Mail - Ritter, Thomas - O
Sign in to continue
Most Visited Forums Virustotal Submit a Sample Malwr
thr1@ITS-ritter-Centos...
Sign in to continue - M...
Mail - Ritter, Thomas -...

Sign in to continue - Mozilla Firefox

file:///tmp/mozilla_thr10/Salary-Receipt.html

Excel

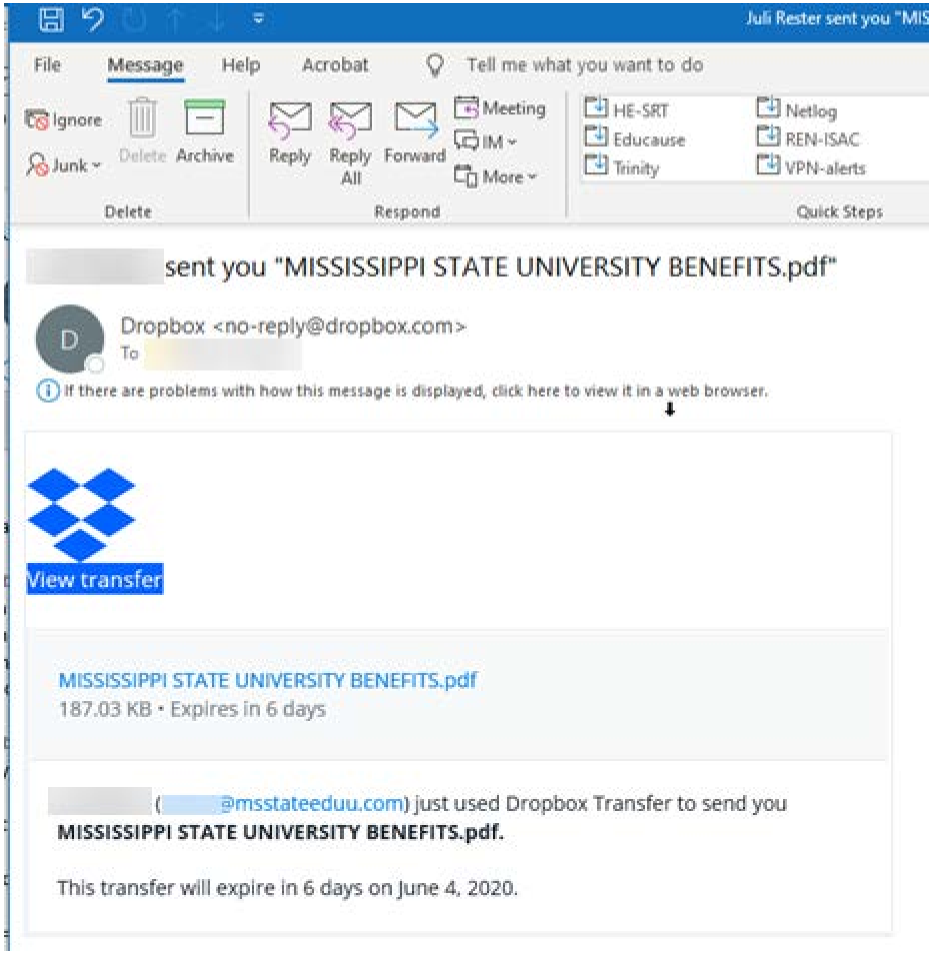
Login with your existing email to view document

txr1@msstate.edu

●●●●●●●●●●●●●●●●●

View Document

Summertime Phishing



[redacted] sent you "MISSISSIPPI STATE UNIVERSITY BENEFITS.pdf"

D Dropbox <no-reply@dropbox.com>
To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

View transfer

MISSISSIPPI STATE UNIVERSITY BENEFITS.pdf
187.03 KB • Expires in 6 days

[redacted] ([redacted]@msstateeduu.com) just used Dropbox Transfer to send you **MISSISSIPPI STATE UNIVERSITY BENEFITS.pdf.**

This transfer will expire in 6 days on June 4, 2020.

Notes

~1500 copies delivered

Hacker did reconnaissance!

Real HRM User with relevant topic!

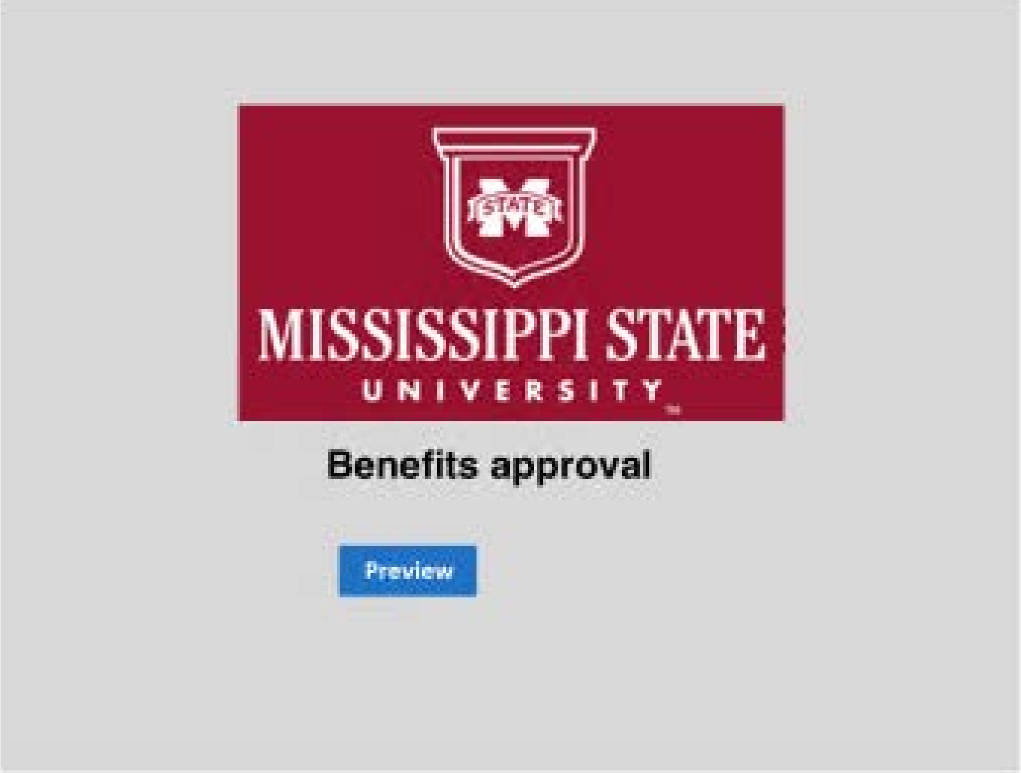
Fake "look-alike" domain

@msstateeduu.com

Simple payload

Came from a real service!

Recent Phishes



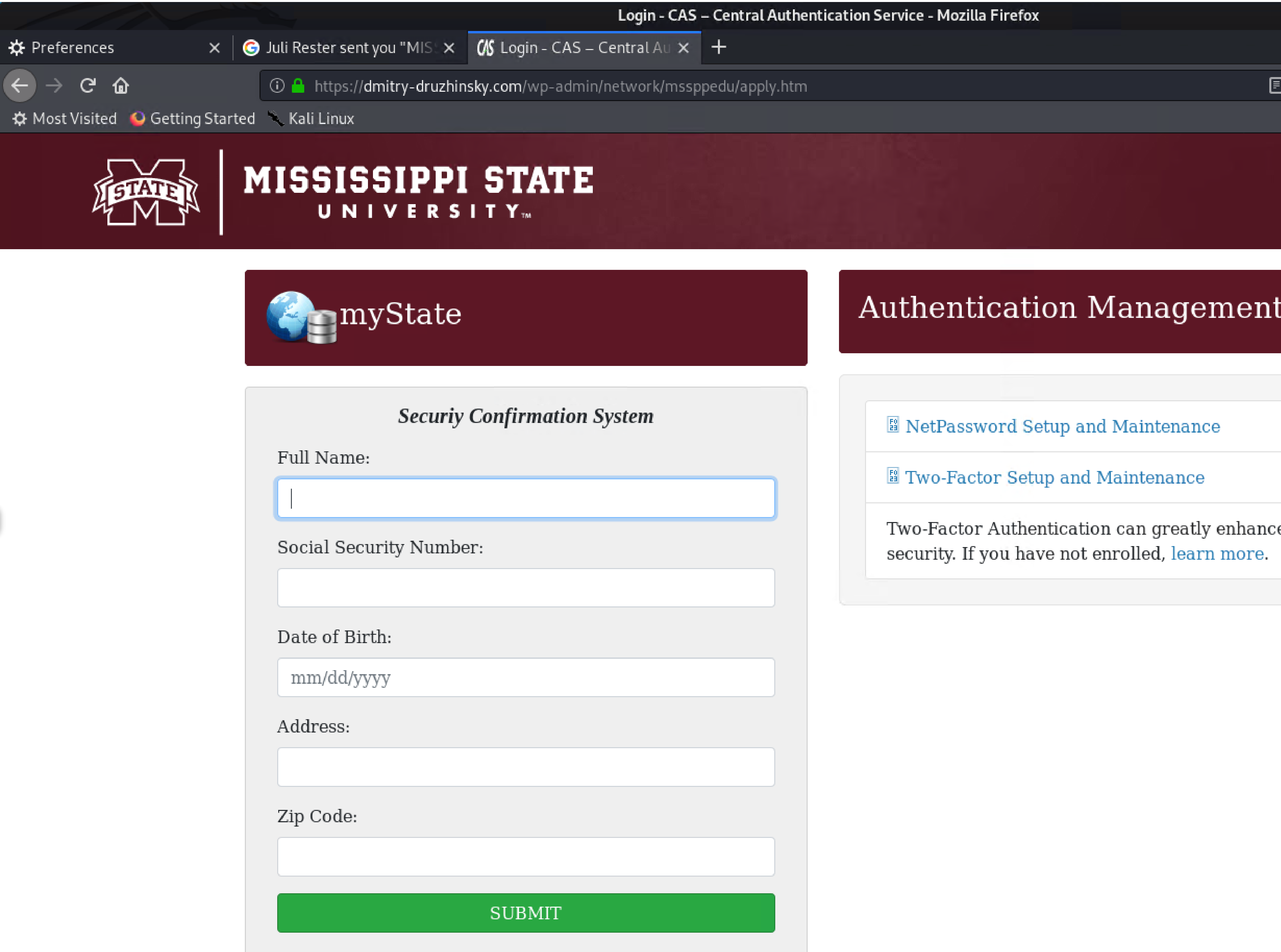
Notes

This is all that was in the payload.

A simple PDF that contained an image and a link. This will not trigger anti-virus until the URL is known to AV vendors.

MSU scans email with two AV products in the cloud before delivery.

Link was quickly blocked but most users were off-campus during covid-19 crisis.


Login - CAS – Central Authentication Service - Mozilla Firefox
Preferences
Juli Rester sent you "MIS
Login - CAS – Central Au
https://dmitry-druzhinsky.com/wp-admin/network/mssppedu/apply.htm
Most Visited
Getting Started
Kali Linux
MISSISSIPPI STATE UNIVERSITY™
STATE

myState

Securiy Confirmation System

Full Name:

Social Security Number:

Date of Birth:

mm/dd/yyyy

Address:

Zip Code:

Authentication Management

NetPassword Setup and Maintenance

Two-Factor Setup and Maintenance

Two-Factor Authentication can greatly enhance
security. If you have not enrolled, learn more.

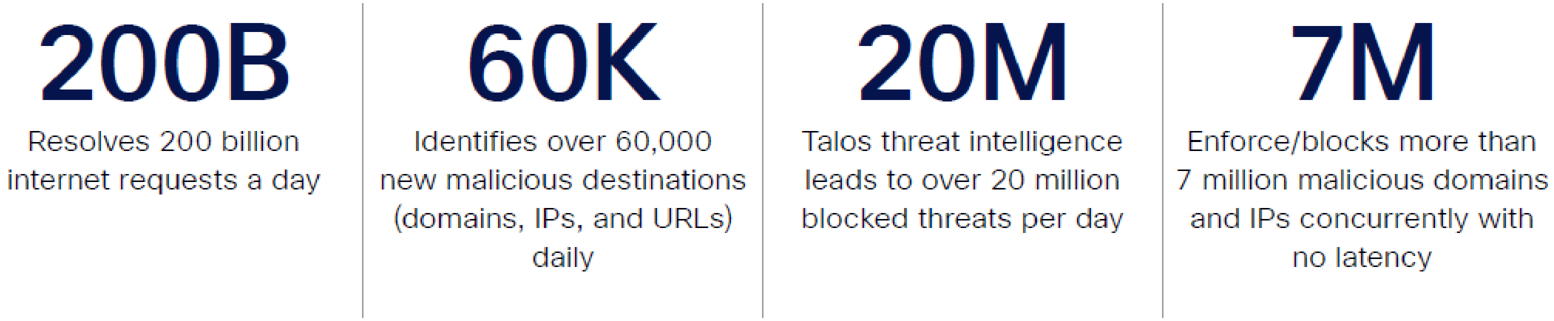
Measures Used to protect users

That email was deleted from O365 mailboxes

- This is only the second time that has ever been done in ITS history.
- Case report forwarded to UPD/FBI/MDITS
- UPD reported 18 victims as of 6/1/2020
- Homegrown “CleanDNS” blocking was of limited use due to off-campus teleworkers even though they were using MSU equipment
- Cisco Umbrella in testing but not deployed to any roaming MSU computers

Cisco Umbrella

- First line of defense for campus
- Enforces security at the Domain Name System (DNS) layer blocking requests to malware, ransomware, phishing and botnet command and control before the connection is established.



200B	60K	20M	7M
Resolves 200 billion internet requests a day	Identifies over 60,000 new malicious destinations (domains, IPs, and URLs) daily	Talos threat intelligence leads to over 20 million blocked threats per day	Enforce/blocks more than 7 million malicious domains and IPs concurrently with no latency

Built into foundation of the internet

Destinations

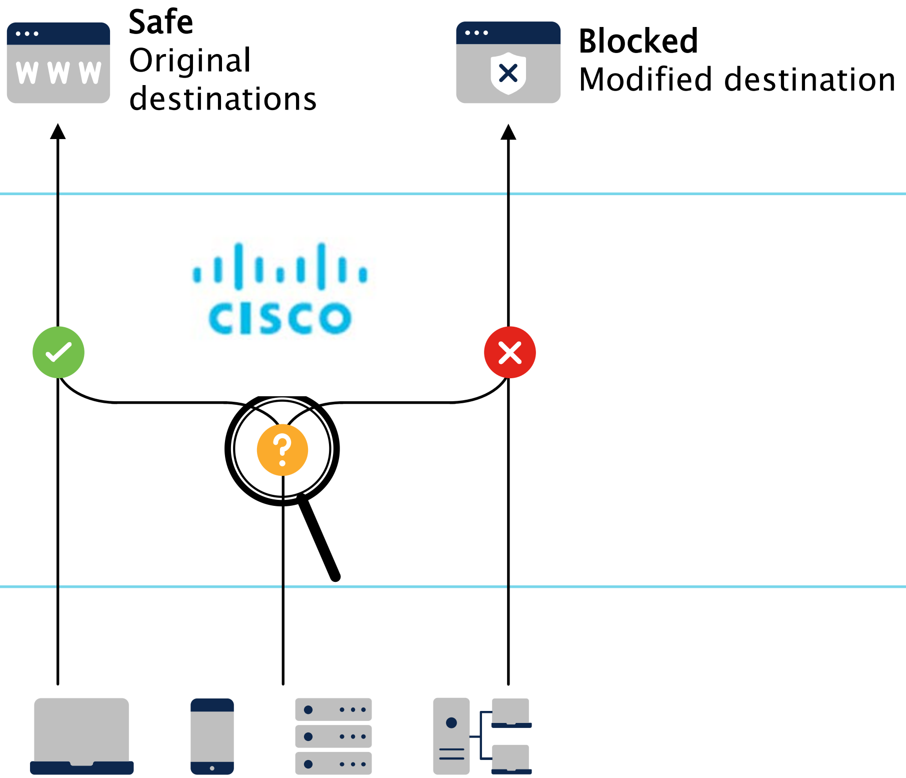
Original destination or block page

Security controls

- DNS and IP enforcement
- Risky domain blocking

Internet traffic

On and off-network



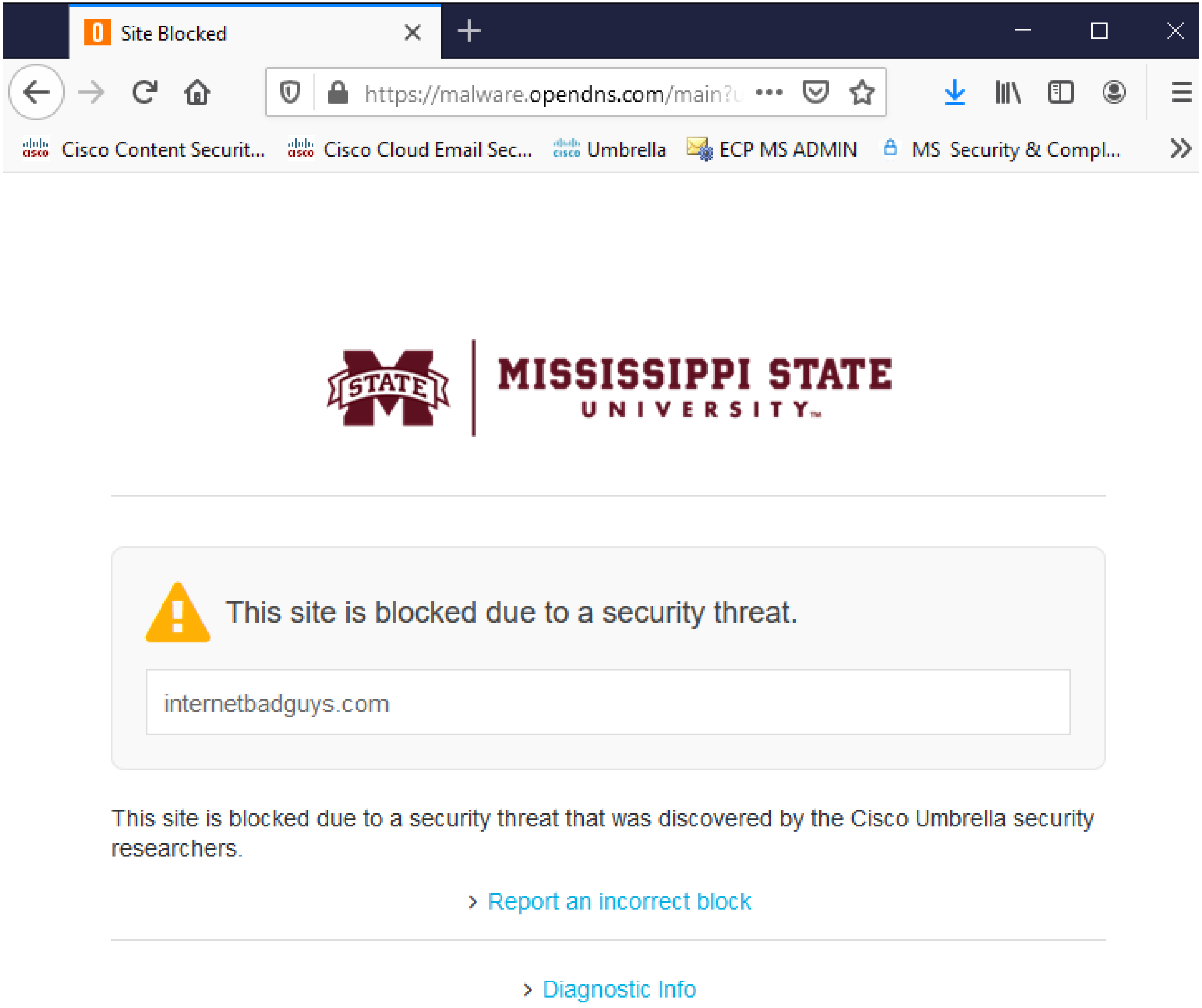
Safe
Original destinations

Blocked
Modified destination

Cisco Umbrella

- Umbrella Blocks
  - Watering hole compromises
  - Malvertising
  - Virus Command and Control Callbacks
  - OpenDNS is now part of Cisco
  - Licensed for MSU Equipment

- Personal Use
  - OpenDNS
  - Quad9 (9.9.9.9)



This site is blocked due to a security threat.

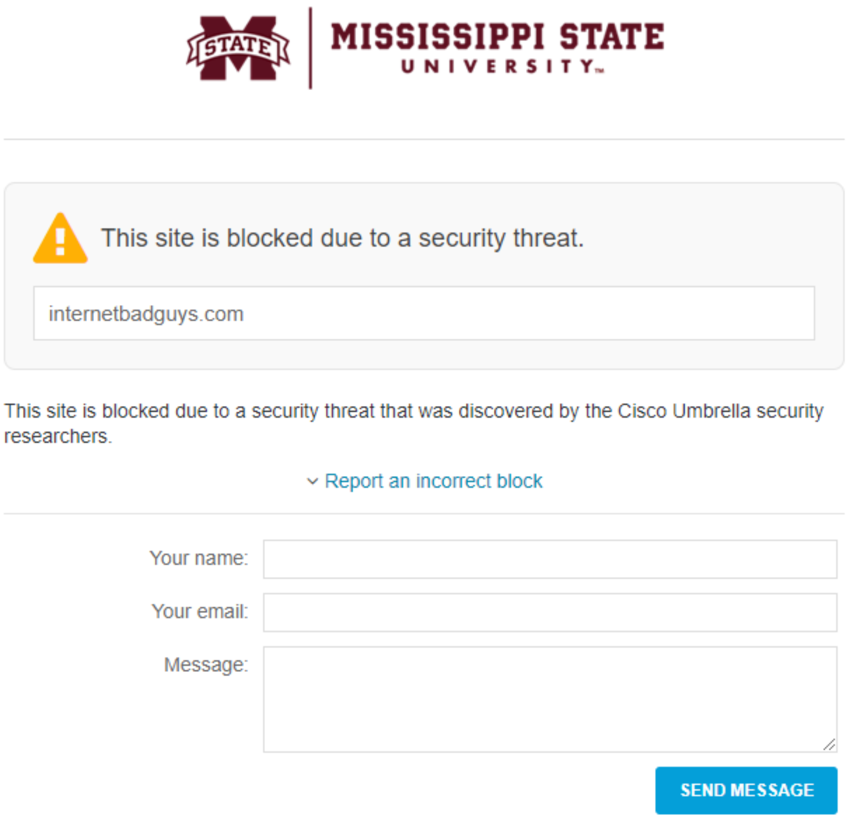
internetbadguys.com

This site is blocked due to a security threat that was discovered by the Cisco Umbrella security researchers.

› Report an incorrect block

› Diagnostic Info

Report a False Positive – Rare but possible



This site is blocked due to a security threat.

internetbadguys.com

This site is blocked due to a security threat that was discovered by the Cisco Umbrella security researchers.

Notes

Block page notifies ITS Service Desk

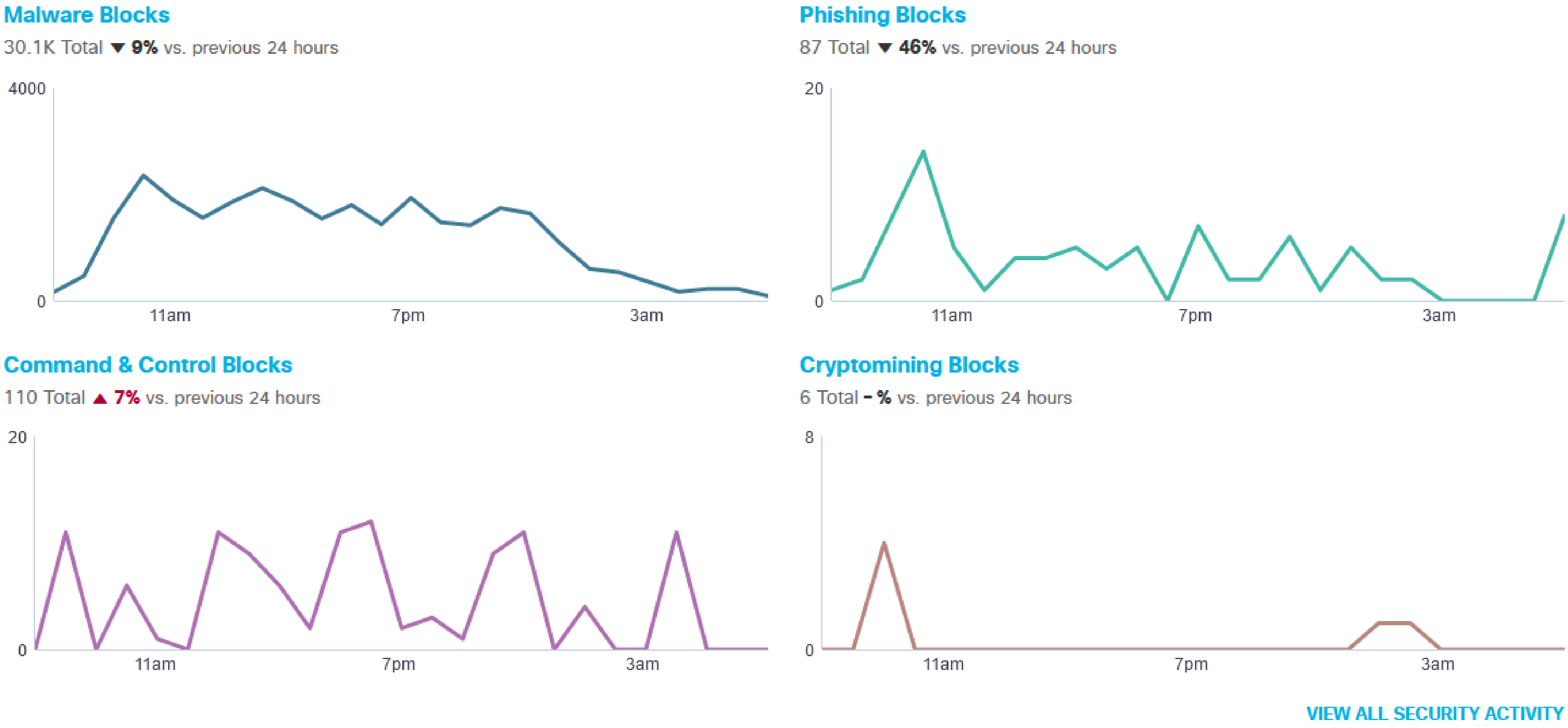
MSU can blacklist specific hostname/phishing sites and it stops access both on campus and roaming systems.

Please report particularly scary or targeted phishing attacks to the ITS Service Desk.

Forward as an attachment to:

servicedesk@msstate.edu

Today's Report



Malware Blocks

30.1K Total ▼ **9%** vs. previous 24 hours

Phishing Blocks

87 Total ▼ **46%** vs. previous 24 hours

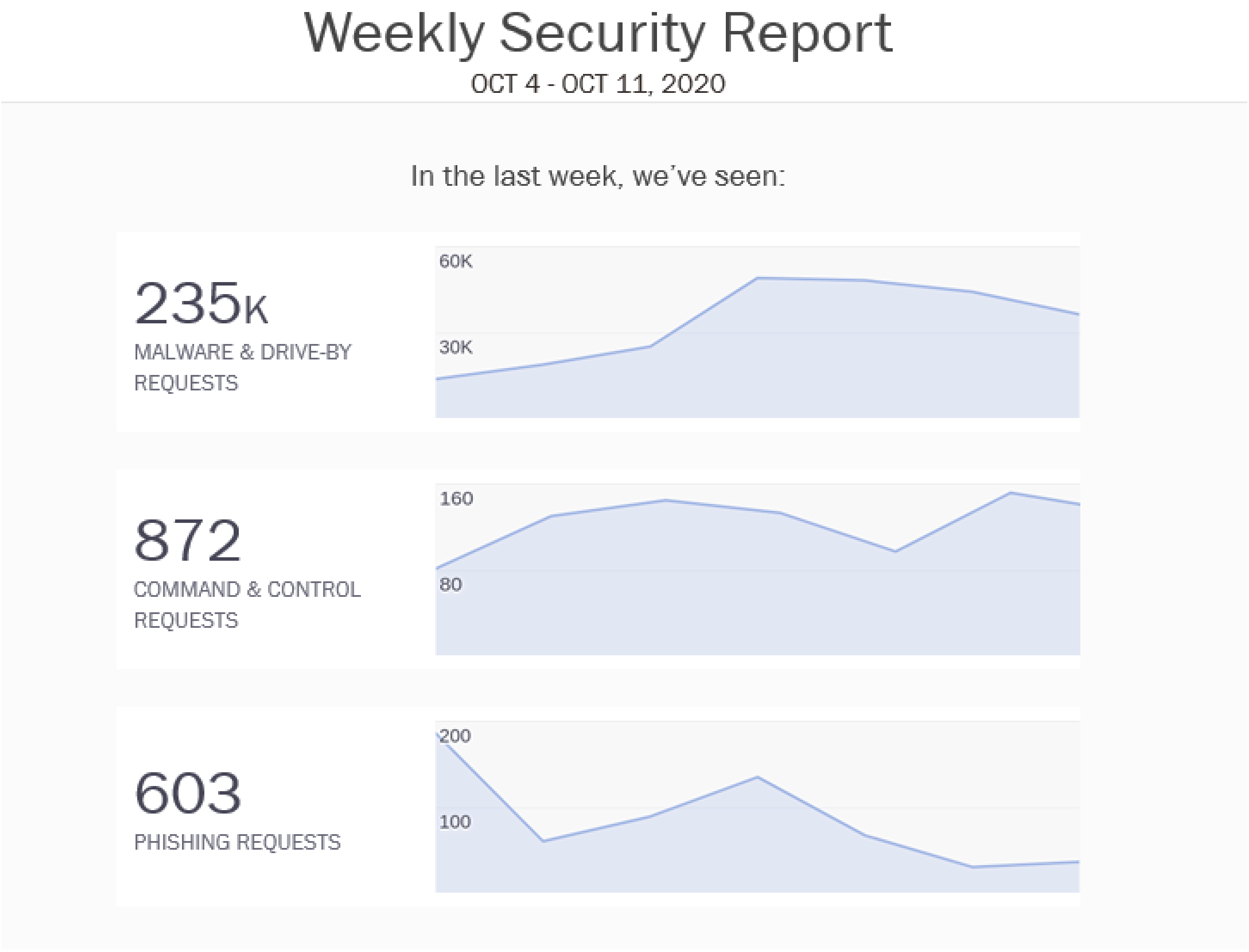
Command & Control Blocks

110 Total ▲ **7%** vs. previous 24 hours

Cryptomining Blocks

6 Total **- %** vs. previous 24 hours

VIEW ALL SECURITY ACTIVITY



Weekly Security Report

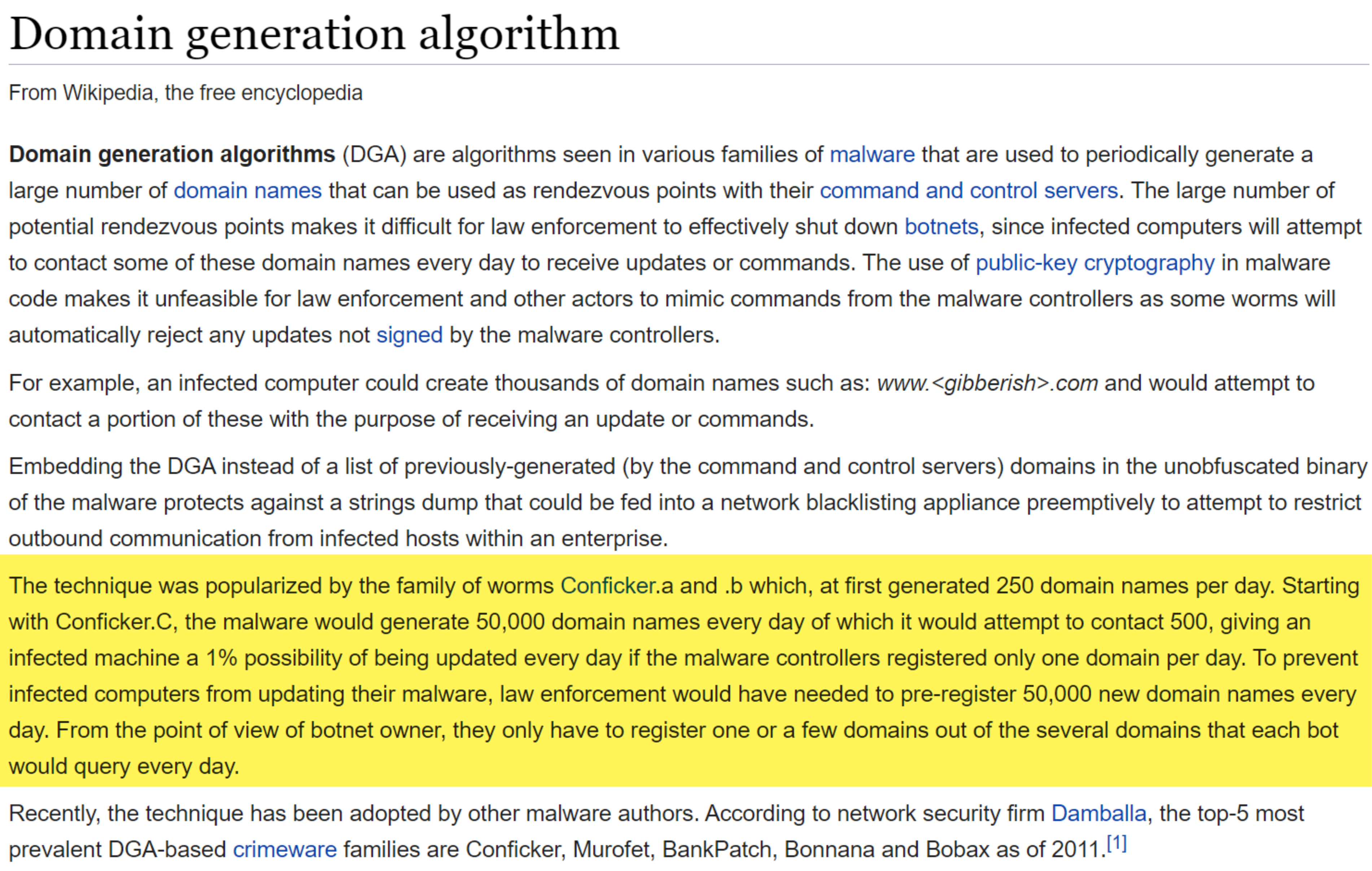
OCT 4 - OCT 11, 2020

In the last week, we've seen:

235K
MALWARE & DRIVE-BY REQUESTS

872
COMMAND & CONTROL REQUESTS

603
PHISHING REQUESTS



Domain generation algorithm

From Wikipedia, the free encyclopedia

Domain generation algorithms (DGA) are algorithms seen in various families of malware that are used to periodically generate a large number of domain names that can be used as rendezvous points with their command and control servers. The large number of potential rendezvous points makes it difficult for law enforcement to effectively shut down botnets, since infected computers will attempt to contact some of these domain names every day to receive updates or commands. The use of public-key cryptography in malware code makes it unfeasible for law enforcement and other actors to mimic commands from the malware controllers as some worms will automatically reject any updates not signed by the malware controllers.

For example, an infected computer could create thousands of domain names such as: *www.<gibberish>.com* and would attempt to contact a portion of these with the purpose of receiving an update or commands.

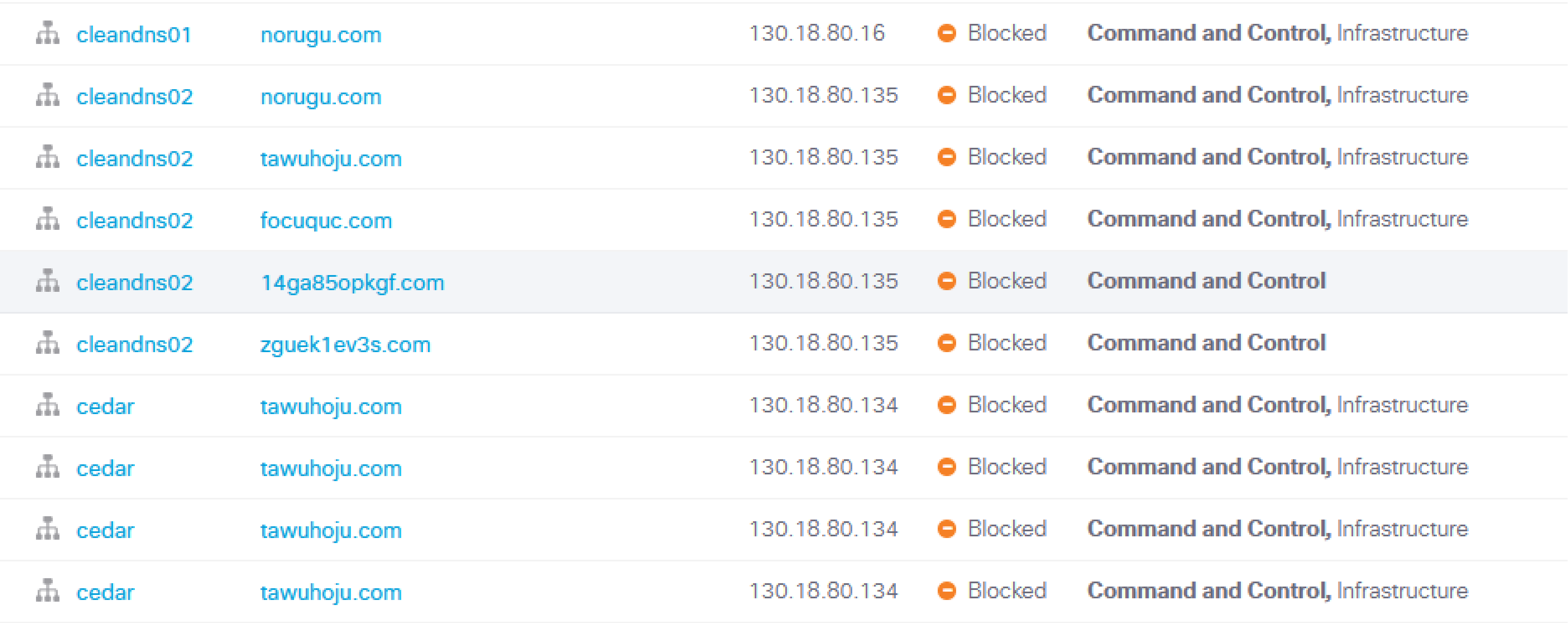
Embedding the DGA instead of a list of previously-generated (by the command and control servers) domains in the unobfuscated binary of the malware protects against a strings dump that could be fed into a network blacklisting appliance preemptively to attempt to restrict outbound communication from infected hosts within an enterprise.

The technique was popularized by the family of worms Conficker.a and .b which, at first generated 250 domain names per day. Starting with Conficker.C, the malware would generate 50,000 domain names every day of which it would attempt to contact 500, giving an infected machine a 1% possibility of being updated every day if the malware controllers registered only one domain per day. To prevent infected computers from updating their malware, law enforcement would have needed to pre-register 50,000 new domain names every day. From the point of view of botnet owner, they only have to register one or a few domains out of the several domains that each bot would query every day.

Recently, the technique has been adopted by other malware authors. According to network security firm Damballa, the top-5 most prevalent DGA-based crimeware families are Conficker, Murofet, BankPatch, Bonnana and Bobax as of 2011.[1]

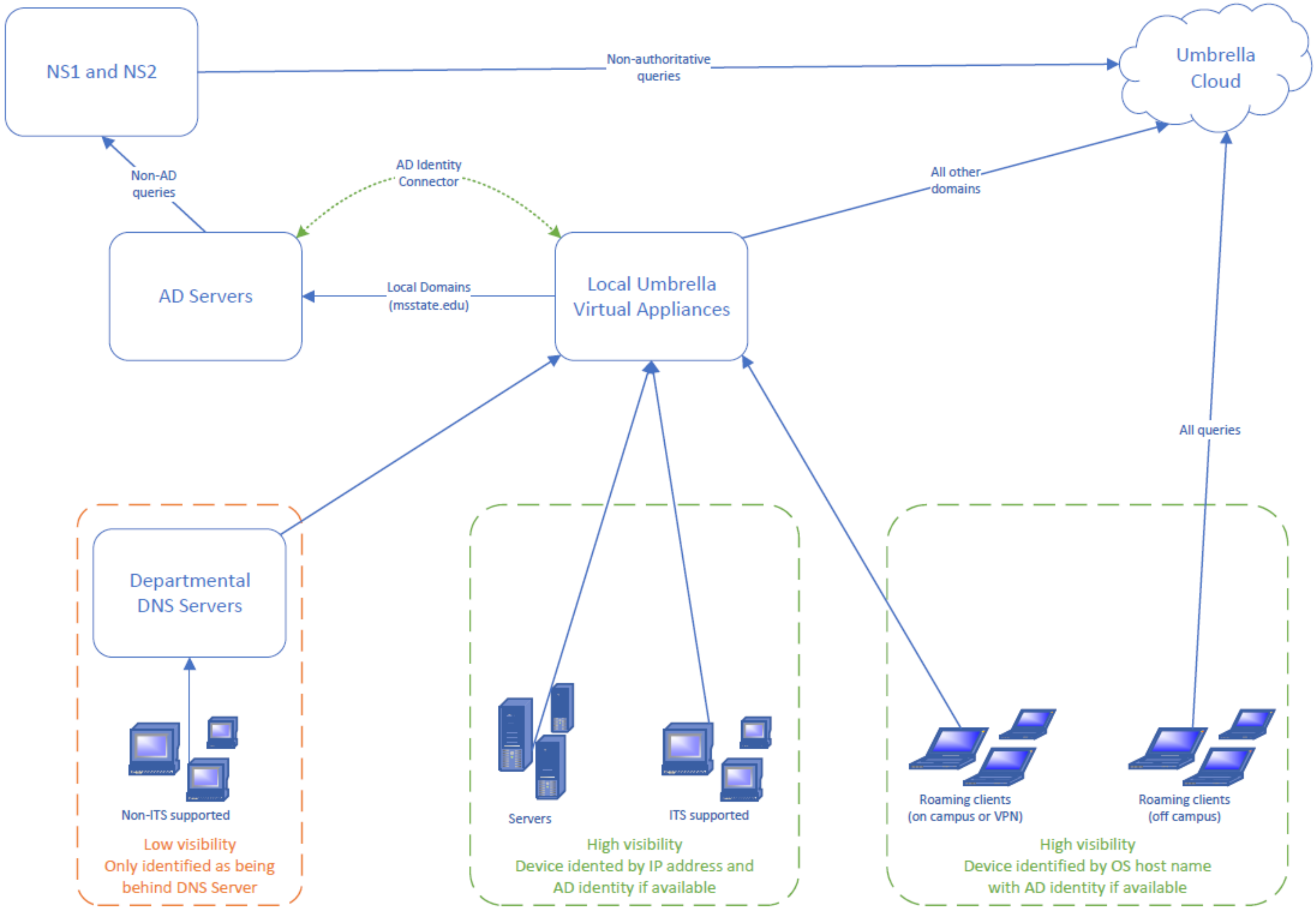
Domain Generation Algorithm

Malware periodically generates Domain Names to make it hard to shutdown a botnet



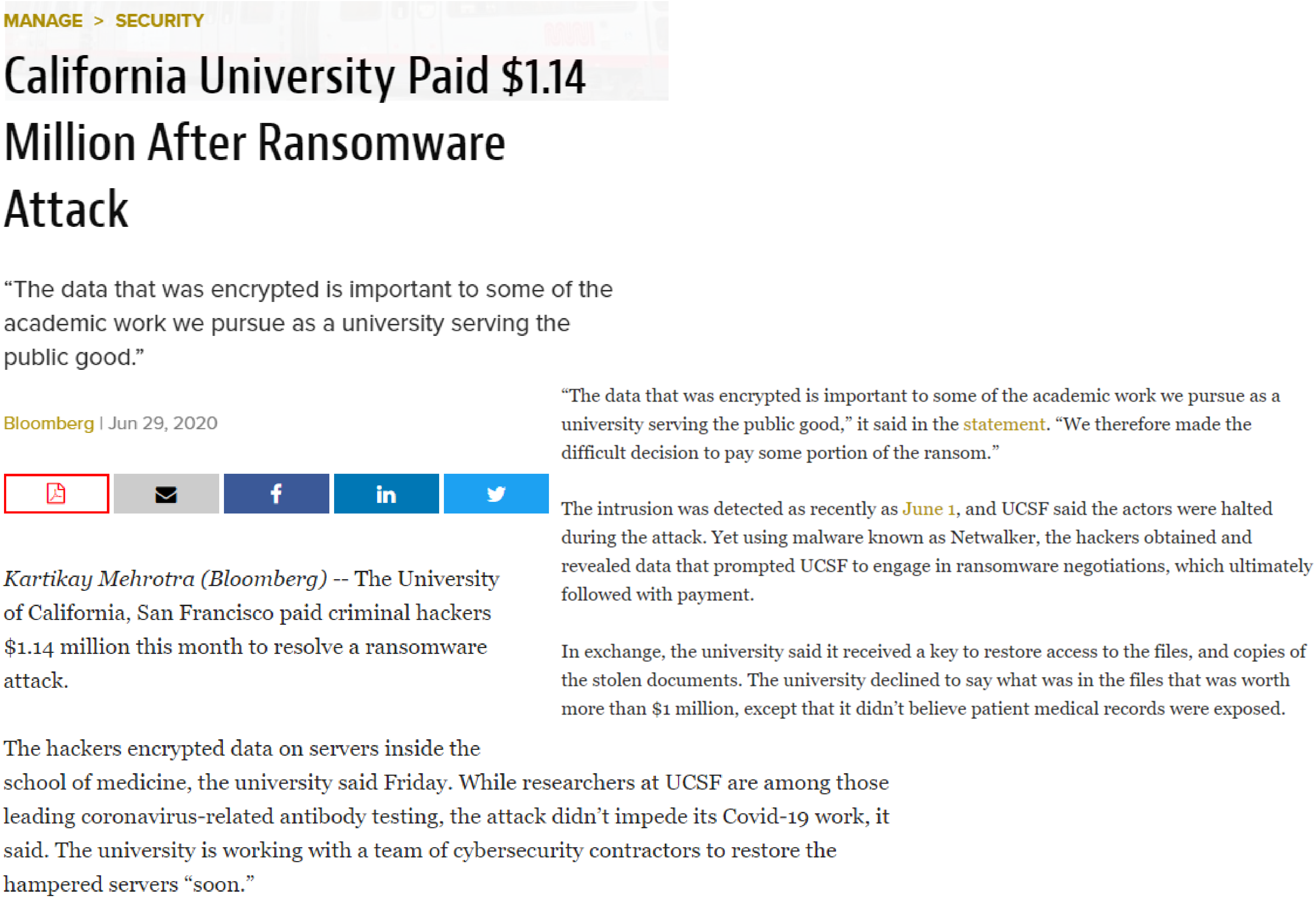
cleandns01	norugu.com	130.18.80.16	Blocked	**Command and Control,** Infrastructure
cleandns02	norugu.com	130.18.80.135	Blocked	**Command and Control,** Infrastructure
cleandns02	tawuhoju.com	130.18.80.135	Blocked	**Command and Control,** Infrastructure
cleandns02	focuquc.com	130.18.80.135	Blocked	**Command and Control,** Infrastructure
cleandns02	14ga85opkgf.com	130.18.80.135	Blocked	**Command and Control**
cleandns02	zguek1ev3s.com	130.18.80.135	Blocked	**Command and Control**
cedar	tawuhoju.com	130.18.80.134	Blocked	**Command and Control,** Infrastructure
cedar	tawuhoju.com	130.18.80.134	Blocked	**Command and Control,** Infrastructure
cedar	tawuhoju.com	130.18.80.134	Blocked	**Command and Control,** Infrastructure
cedar	tawuhoju.com	130.18.80.134	Blocked	**Command and Control,** Infrastructure

MSU Umbrella/DNS Architecture


NS1 and NS2
Non-authoritative queries
Umbrella Cloud
Non-AD queries
AD Identity Connector
All other domains
AD Servers
Local Domains (msstate.edu)
Local Umbrella Virtual Appliances
All queries
Departmental DNS Servers
Non-ITS supported
Low visibility
Only identified as being behind DNS Server
Servers
ITS supported
High visibility
Device idented by IP address and AD identity if available
Roaming clients (on campus or VPN)
Roaming clients (off campus)
High visibility
Device identified by OS host name with AD identity if available

Changing security landscape....

- Less “hobby” hackers more nation-state
- Less “fame” driven, more cybercrime
- Less “visible” behavior, more stealth
- More attacks, more ransomware money, more need for security and user awareness



MANAGE > SECURITY

California University Paid $1.14 Million After Ransomware Attack

“The data that was encrypted is important to some of the academic work we pursue as a university serving the public good.”

Bloomberg | Jun 29, 2020

Kartikay Mehrotra (Bloomberg) -- The University of California, San Francisco paid criminal hackers $1.14 million this month to resolve a ransomware attack.

The hackers encrypted data on servers inside the school of medicine, the university said Friday. While researchers at UCSF are among those leading coronavirus-related antibody testing, the attack didn’t impede its Covid-19 work, it said. The university is working with a team of cybersecurity contractors to restore the hampered servers “soon.”

“The data that was encrypted is important to some of the academic work we pursue as a university serving the public good,” it said in the statement. “We therefore made the difficult decision to pay some portion of the ransom.”

The intrusion was detected as recently as June 1, and UCSF said the actors were halted during the attack. Yet using malware known as Netwalker, the hackers obtained and revealed data that prompted UCSF to engage in ransomware negotiations, which ultimately followed with payment.

In exchange, the university said it received a key to restore access to the files, and copies of the stolen documents. The university declined to say what was in the files that was worth more than $1 million, except that it didn’t believe patient medical records were exposed.

Teleworking Requires an Increased Security Awareness

- Home and Wireless Security
- Situational Awareness
- Physical Protection
- Data Security

Home and Wireless Security

- Enable network encryption (WPA2 or WPA3)
- Make your wireless network password strong and keep it confidential
- Keep your wireless router patched and enable auto update wherever possible
- Enable the built-in firewall that generally comes with most routers

Situational Awareness

- Don’t talk about confidential work in a public place
- Avoid over the shoulder surfers, turn monitors away from windows, drop the shades at night, etc…
- Keep non-workers away from laptops/mobile devices – Lock screen! (Windows-L shortcut)
- BEWARE the Pandemic/Business Email phishing

Physical Protection

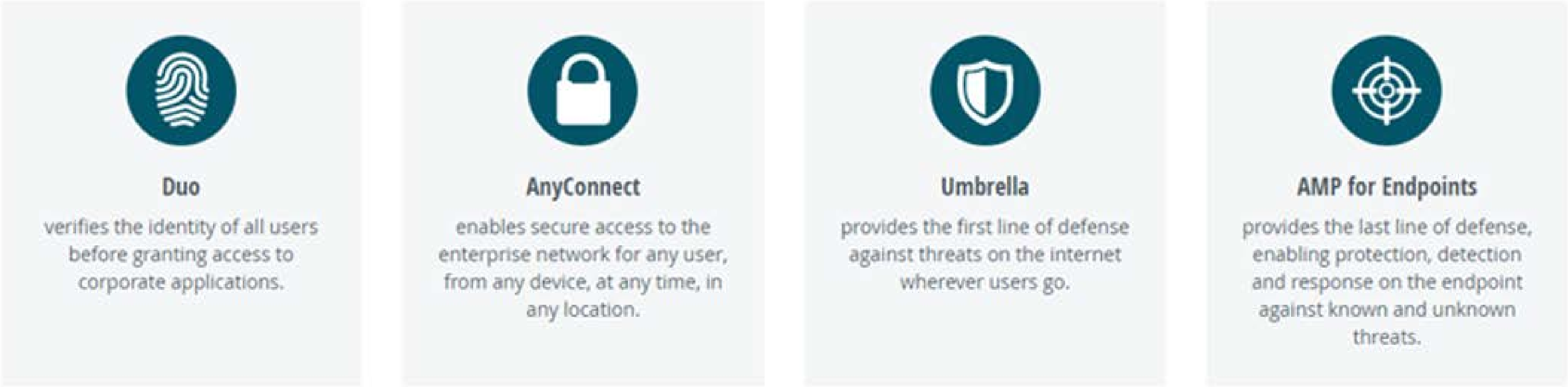
- Lock your doors!
- Don’t leave your laptop in the car, etc.
- Don’t leave the laptop in the sun, outdoors, edge of the concrete pool....
- Encrypt your laptop so if it is stolen it’s just a theft, not a data breach

Ponemon Institute's Cost of a Data Breach Report, an annual compendium of data breach trends that over the years has become a barometer of sorts for the information security industry, in 2020, data breaches on average cost $3.86 million

Data Security

- Install the Cisco Umbrella Roaming Client
- Leave work at work and Remote Desktop via the VPN for access if applicable
- Don’t conduct MSU business via personal accounts whether in email or dropbox, etc.
- Don’t allow family members to use work systems
- Use University supported Microsoft 365 (2fa) cloud services. Share files with CAUTION.
- Think before you click!

Cisco Software Protection for MSU



Duo

verifies the identity of all users before granting access to corporate applications.

AnyConnect

enables secure access to the enterprise network for any user, from any device, at any time, in any location.

Umbrella

provides the first line of defense against threats on the internet wherever users go.

AMP for Endpoints

provides the last line of defense, enabling protection, detection and response on the endpoint against known and unknown threats.

- Integrated threat investigation
- Cisco Threat Response

Cisco Talos

- Largest non-government threat intelligence organization on the planet
- 250+ full-time threat researchers and data scientists
- Blocks 20 billion threats per day
- The huge volume of traffic on Cisco means Talos can see more and respond with blocking and analysis

Questions?
General Discussion