MITSloan MANAGEMENT

INTERDISCIPLINARY
CONSORTIUM
for IMPROVING
CRITICAL
INFRASTRUCTURE
CYBERSECURITY

$(IC)^3$

Interview: "The real and growing threat of cyber crime to corporations" CNBC Cambridge Cyber Summit

Stuart Madnick

Working Paper CISL# 2016-17

September 2016

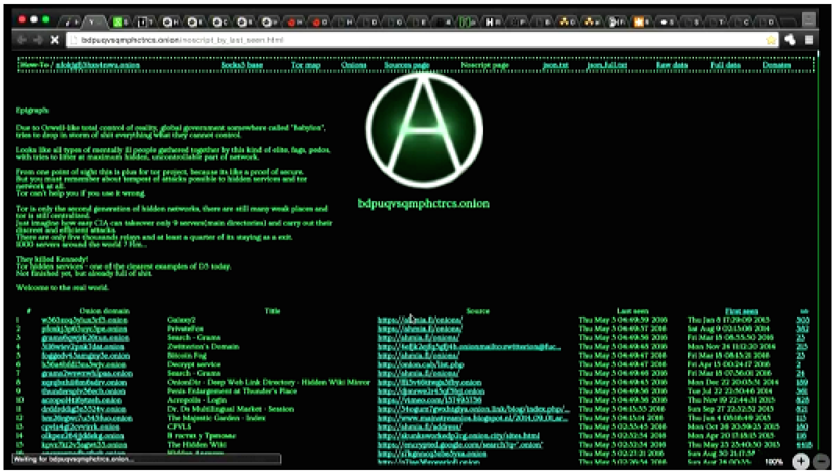
Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

The real and growing threat of cyber crime to corporations

73 SHARES

Stuart Madnick, MIT professor

CNBC



bdpuqvsqmphctrcs.onion/noscript_by_last_seen.html

How-To / [illegible].onion | Socks5 base | Tor map | Onions | Sources page | Noscript page | json.txt | json_full.txt | Raw data | Full data | Donate

Epigraph:

Due to Orwell-like total control of reality, global government somewhere called "Babylon", tries to drop in storm of shit everything what they cannot control.

Looks like all types of mentally ill people gathered together by this kind of elite, fags, pedos, with tries to filter at maximum hidden, uncontrollable part of network.

From one point of sight this is plus for tor project, because its like a proof of secure. But you must remember about tempest of attacks possible to hidden services and tor network at all.
Tor can't help you if you use it wrong.

Tor is only the second generation of hidden networks, there are still many weak places and tor is still centralized.
Just imagine how easy CIA can takeover only 9 servers(main directories) and carry out their discreet and efficient attacks.
There are only five thousands relays and at least a quarter of its staying as a exit.
1000 servers around the world ? Hm...

They killed Kennedy!
Tor hidden services - one of the clearest examples of DS today.
Not finished yet, but already full of shit.

Welcome to the real world.

bdpuqvsqmphctrcs.onion

#	Onion domain	Title	Source	Last seen	First seen	[illegible]
1	[illegible].onion	Galaxy2	https://ahmia.fi/onions/	Thu May 5 04:49:59 2016	Thu Jan 8 17:29:09 2015	303
2	[illegible].onion	PrivateFox	https://ahmia.fi/onions/	Thu May 5 04:49:57 2016	Sat Aug 9 02:15:08 2014	382
3	[illegible].onion	Search - Grams	http://ahmia.fi/onions/	Thu May 5 04:49:56 2016	Fri Mar 18 08:55:50 2016	25
4	[illegible].onion	Zwitterion's Domain	[illegible]	Thu May 5 04:49:48 2016	Mon Nov 24 11:02:30 2014	205
5	[illegible].onion	Bitcoin Fog	http://ahmia.fi/onions/	Thu May 5 04:49:47 2016	Fri Mar 18 08:15:21 2016	25
6	[illegible].onion	Decrypt service	http://onion.cab/list.php	Thu May 5 04:49:47 2016	Fri Apr 15 00:24:17 2016	2
7	[illegible].onion	Search - Grams	http://ahmia.fi/onions/	Thu May 5 04:49:46 2016	Fri Mar 18 07:56:08 2016	24
8	[illegible].onion	OnionDir - Deep Web Link Directory - Hidden Wiki Mirror	[illegible].onion	Thu May 5 04:49:45 2016	Mon Dec 22 20:05:51 2014	159
9	[illegible].onion	Penis Enlargement at Thunder's Place	[illegible].onion	Thu May 5 04:49:38 2016	Tue Jul 22 21:50:46 2014	361
10	[illegible].onion	Acropolis - Login	https://vimeo.com/151993158	Thu May 5 04:49:38 2016	Thu Nov 19 22:44:31 2015	620
11	[illegible].onion	Dr. D's Multilingual Market - Session	[illegible]	Thu May 5 04:15:33 2016	Sun Sep 27 22:32:52 2015	621
12	[illegible].onion	The Majestic Garden - Index	[illegible]	Thu May 5 04:15:04 2016	Thu Jun 4 08:08:49 2015	115
13	[illegible].onion	CPVLS	http://ahmia.fi/address/	Thu May 5 02:55:45 2016	Mon Oct 26 20:59:25 2015	160
14	[illegible].onion	[illegible]	[illegible]	Thu May 5 02:52:54 2016	Mon Apr 20 17:18:15 2015	136
15	[illegible].onion	The Hidden Wiki	[illegible]	Thu May 5 02:52:34 2016	Thu May 21 23:40:30 2015	6108
16	[illegible]	Hidden [illegible]	[illegible].onion	Thu May 5 02:21:21 2016	Sun Aug 30 21:17:59	[illegible]

Waiting for bdpuqvsqmphctrcs.onion...

The cyber threat is real.

If you have control of valuable assets, including trillions of dollars of transactions, as The Society for Worldwide Interbank Financial Telecommunications (SWIFT) does, your company will be attacked. It's a matter of when, not if, it will happen. That means you need to develop a sophisticated and multi-faceted approach to cyber-security.

Only a few years ago, corporate cyber-security might have been limited to installing the latest software patch—an activity on a par with, say, facilities management.

However, given the increasing number and magnitude of cyber-crimes, as well as new types of threats, cyber-security now requires a coordinated effort between companies, government agencies and advanced academics with cutting edge insights into the future of technology. In a networked world, no one can afford to go it alone.

"It is up to senior business leaders to take the lead in protecting their organizations."

-Stuart Madnick, Director, MIT's Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity

While there still may be lone-wolf high school students hacking into systems in their spare time, most of the current serious attacks are initiated through use of an elaborate cyber-crime ecosystem. There, techies create cyber weapons that cybercriminals can buy on the "dark web" –often for remarkably low costs. Recently it has been reported that cyber weapons developed by the NSA were stolen and are up for sale.

Cybercrime poses a real and persistent threat to business, government and financial institutions. The February 2016 theft of $81 million dollars from the Bank of Bangladesh's holdings at the New York Federal Reserve via the SWIFT network serves as an important reminder of how effective and damaging these attacks can be. The thieves used the bank's own computers to make what appeared to be legitimate transfers of millions of dollars.

Attacks such as these are increasingly multi-pronged and require extensive knowledge of the organizations and systems being attacked.

For example: After the malware attack on the Bangladesh Central Bank sent the fund requests, it deleted the database record of the transfers, took steps to prevent confirmation messages from revealing the theft, and even altered the reports that were sent to the printer. Similar elaborate schemes were used in the December 2015 attack on Ukraine's power grid.

Although all the details of the Bangladesh event are not known, we do know that 50-80 percent of all cyber-attacks are aided or abetted by insiders, most commonly by an email message that asks a relevant party to click a link or open an attachment.

It is highly likely that almost everyone has received one of these Phishing attempts. Some are the fairly obvious: "I am a Nigerian Prince with millions to give you." These have a 1-2 percent success rate. Meanwhile, the more subtle "you have exceeded your email quota and you need to take this action to continue getting email"–can have a 10 percent success rate.

But, the real challenge is Spear Phishing, where success rates can exceed 70 percent. These are carefully crafted messages that appear to be coming from trusted individuals, such as a known executive in your company, and make use of detailed knowledge about you and your job.

Sophisticated threats and attacks such as these require a multi-pronged response. And while each organization will fashion its own customized response, we believe the all companies, institutions and government agencies should think holistically e2e, end-to-end.

It is up to senior business leaders to take the lead in protecting their organizations; and in the dark and complex world of cybercrime that can only be accomplished by working together with government, industry, and academia.