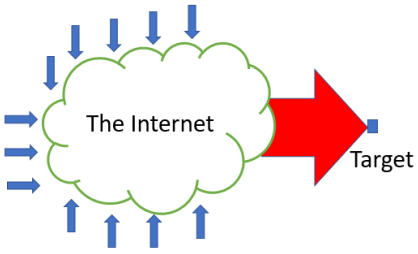
TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint — *April 2017 , Volume 1 Issue 3*

IoT Makes DDOS Much Worse

By Peter Aggus

The number of cyberattacks grew by 75% last year. The biggest (so far) 'Distributed Denial of Service', or DDoS, attack on internet company Dyn occurred last October and left customers of online services such as Netflix, Amazon, Twitter and Reddit without service. Tens of millions of Internet of Things (IoT) and smart home devices were recruited and created attack traffic of over 600 Gbps of data. This level of attack can be easily created. Your IoT devices could be enslaved and lying dormant without your knowledge. How can you avoid being a part of the problem?



Hundreds of thousands of unsuspecting botnet hosts each with 10-10,000 IoT slave devices.

Inside

- By Lee-Ann Dittrich

When Isaac Asimov invented the 3 Laws of Robotics, they were intended as a foundation for his fictional stories. Everyone who read his work knew that humanity needed something similar. Happily, the biggest names in tech have now created a real world version – the Asilomar AI Principles.

- By John Glover

43,000 attendees of RSA 2017 in San Francisco learned some important InfoSec lessons in February. Here are the most important, including a critical, low-tech lesson.

- By Ellen Koskinen-Dodgson

Computers used to be huge, with lots of cabinets filling a big room. Computers shrank and became distributed and personal, but we still needed computer rooms with racks of servers and storage arrays. Next it seemed like everything was becoming virtualized, either on site or in the cloud. As we're getting used to the next big paradigm - 'Convergence', along comes 'Hyperconvergence'. Is this the new nirvana?

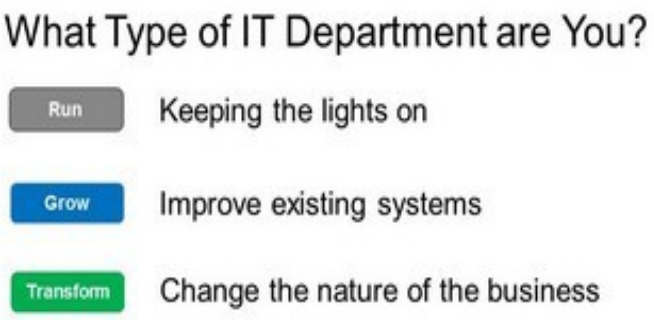
The ROI on IT Assessments

Our clients have hired us to conduct an assessment of their IT operations for a variety of reasons including:

- Investigating reliability problems
- Assessing customer service levels
- Benchmarking costs
- Assessing staffing levels and skills
- Assessing IT Process Maturity

More Information

Contact Ellen for a complimentary copy of **IT Assessments 123**.
ellen@tmcconsulting.ca or 604-506-2905



 ISSN 2369-663X

IoT Makes DDOS Much Worse

By Peter Aggus

The number of cyberattacks grew by 75% last year. The biggest (so far) 'Distributed Denial of Service', or DDoS, attack on internet company Dyn occurred last October and left customers of online services such as Netflix, Amazon, Twitter and Reddit without service. Tens of millions of Internet of Things (IoT) and smart home devices were recruited and created attack traffic of over 600 Gbps of data. This level of attack can be easily created. Your IoT devices could be enslaved and lying dormant without your knowledge. How can you avoid being a part of the problem?

Profile of an Attack

Around 7:00 a.m. on Friday October 21, the first data assault began—affecting Dyn's East Coast customers. Their Network Operations Center (NOC) team was able to stop the attack in about two hours.

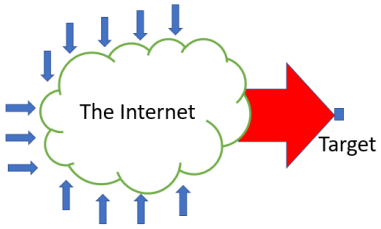
After noon, another attack began and it affected customers on a global scale. Dyn was able to mitigate that attack within the hour.

A third attack was stopped before it greatly affected any customers. These attacks involved rogue data traffic in excess of 600 Gbps.

Rise of the Botnet

The creators of all this traffic were millions of devices with a small amount of processing power and access to the internet—devices referred to as 'bots'. They are simply programmed to send endless streams of data to a target host with each transmission requiring a response .

Recruiting these bots was done by a piece of malware known as Mirai. This program can infect any computer in the usual ways for viruses. Once active on a network host it looks for IoT devices and reprograms them for its own purposes.



Hundreds of thousands of unsuspecting botnet hosts each with 10-10,000 IoT slave devices.

The Unwilling Host

Creating botnets like this requires two conditions. The first is a host computer to infect—typically with an e-mail scare message that results in a user clicking the link. The second is the presence of other processors on the same network—Mirai looks for IoT devices configured with default passwords which it can reprogram.

Once set up, the botnet remains dormant and waiting. The host will keep checking for requests, and when told to, it will issue a blast of data for a defined time against a specified target. Botnets are for rent on the internet if you know where to look – like a digital 'assassin for hire'.

What You Need To Do

You need to look at the role your infrastructure might be playing in being a rogue botnet.

Track your outgoing data traffic and if it is a lot more than it should be, find out where the traffic is coming from.

Make sure your IoT passwords are not the published defaults and get the software patches up to date. It may only be a thermostat but it could easily become a 'bot'.

Note that this is not your usual firewall issue. This is how cyber terrorism is inserting malicious code inside the firewall-protected shell. This is both how the original Trojan Horse worked and how the Stuxnet virus allegedly infected Iranian nuclear centrifuges.

Liability

These DDoS attacks start somewhere and your infrastructure might easily be a contributor. We have yet to see a case made against a botnet host for damages but it is sure to come.

Ignorance is not a defence – the standard for protection against liability will be 'due diligence'.

This article is reproduced from the April 2017 edition of ***TMC's Advisor***

Peter, as an engineer & technology management consultant, has developed innovative & cost-effective solutions for clients in many industries.

The 3 Laws of Robotics Become …

By Lee-Ann Dittrich

When Isaac Asimov invented the 3 Laws of Robotics, they were intended as a foundation for his fictional stories. Everyone who read his work knew that humanity needed something similar. Happily, the biggest names in tech have now created a real world version – the Asilomar AI Principles.

Asilomar AI Principles

In January 2017 the Future of Life Institute brought together 150 AI academic and industry researchers as well as thought leaders in economics, law, ethics, and philosophy to discuss beneficial Artificial Intelligence.

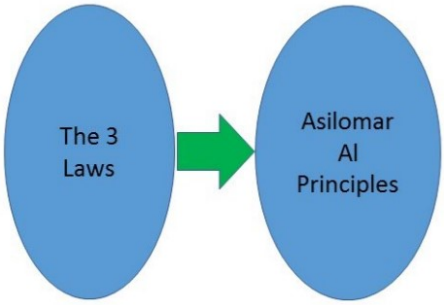
They developed 23 principles as guidance for development of the technology, itemized here, edited for brevity.

Research Issues

1. Research goal - create only beneficial intelligence.
2. Investments should be paired with funding for research on ensuring beneficial use.
3. There should be constructive exchange between AI researchers and policy-makers.
4. Foster a culture of cooperation, trust, and transparency among researchers and developers.
5. Avoid corner-cutting on safety standards during development.

Ethics and Values

6. AI systems should be verifiably safe and secure throughout their operational lifetime, where applicable and feasible.
7. If an AI system causes harm, it should be possible to ascertain why.



8. Any involvement by an autonomous system in judicial decision-making should provide a explanation that is satisfactory to a competent human authority.
9. Designers and builders share responsibility in the moral implications of AI use, misuse, and actions.
10. Highly autonomous AI systems should be designed so that their goals and behaviors align with human values.
11. AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.
12. People should have the right to access, manage and control the data they generate.
13. The use of personal data should not unreasonably curtail people's real or perceived liberty.
14. Benefit and empower as many people as possible
15. Economic prosperity created by AI should benefit all of humanity
16. Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.
17. Respect and improve the social and civic processes on which the health of society depends.
18. Avoid an arms race in lethal autonomous weapons.

Longer-term Issues

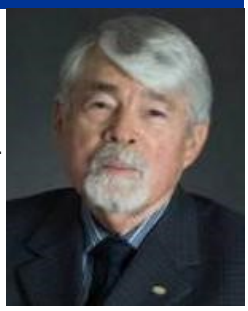
19. Assume no limit to AI capability
20. As AI impact can be profound, manage with care and resources
21. Risk Mitigation efforts should match expected impact.
22. Systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.
23. Superintelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity.

This article is reproduced from the April 2017 edition of ***TMC's Advisor***

Lee-Ann is a researcher and business analyst who oversees benchmarking studies.

Cyber Security Wisdom RSA 2017

By John Glover



43,000 attendees of RSA 2017 in San Francisco learned some important InfoSec lessons in February. Here are the most important, including a critical, low-tech lesson.

Origins

RSA, a US network security company, named after the RSA public key cryptography algorithm which was named after the initials of its co-founders, Ron Rivest, Adi Shamir and Leonard Adleman.

1. Web Services

First, employees completely bypass the IT department and create their own storage and other services. Worse, there's no actual certainty that apps are connecting to the expected entity, or if a man-in-the-middle has stepped in.

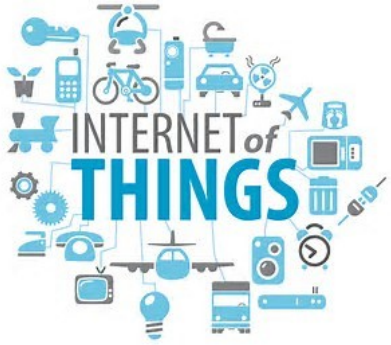
2. Virus/Spam

Your Antivirus is getting less and less effective. Proactive detection rates have dropped from about 80% down to 67-70% over approximately 9 months.

One in 200 emails with malicious attachments makes it through your spam filter. That puts the potential for malware making it into your users' inbox VERY REAL... every day.

3. Ransomware

Ransomware heads the list of deadly attacks. SANS Institute's Ed Skoudis said the rise in ransomware was the



top IT security threat. "We've seen this bring down a whole network of file servers and we expect many more attacks". Ed's advice is to limit permission for network shares to only those jobs that require it. And of course, train your users within an inch of their lives.

4. IRS Top Concerns

Phishing leads the IRS Dirty Dozen of scams. CEO Fraud / W-2 tax form scams are a close second.

5. Phone Scams

Users need to know that when they pick up the phone, the person on the other end might be a criminal hacker that tries to manipulate them into getting access to the network.

They impersonate "Tech Support" and ask for a password, or pretend to solve technical problems which allows them to compromise the workstation.

6. Internet of Things

Both consumer and commercial devices are using wireless protocols to connect to each other and the internet, with vendors rushing products to market without proper security features.

Last Line of Defense

Employees are your last line of defense - an additional security layer when (not if) attacks make it through all of your defenses. Preach the nature of connectedness.

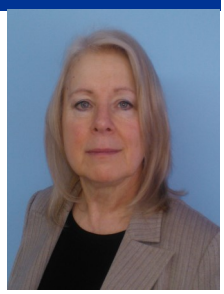
Employees need to be trained to change default passwords and disable remote access for all devices, particularly IoT devices. If your organization has anything to do with critical infrastructure, users need to do fire drills so they are prepared for any kind of attack.

High-risk users need to face simulated attacks using email, phone and text to inoculate them.

This article is reproduced from the April 2017 edition of ***TMC's Advisor***

John Glover assists national and international clients with governance, IT systems compliance auditing, IT risk assessment, information policy formulation and PCI data security.

The Road to Hyperconverged



By Ellen Koskinen-Dodgson

Computers used to be huge, with lots of cabinets filling a big room. Computers shrank and became distributed and personal, but we still needed computer rooms with racks of servers and storage arrays. Next it seemed like everything was becoming virtualized, either on site or in the cloud. As we're getting used to the next big paradigm - 'Convergence', along comes 'Hyperconvergence'. Is this the new nirvana?

Old School

When it all began, the components of hardware needed to make a CPU were split into multiple cabinets to make the size manageable.

Desktop

Electronics progressed to where most functions could fit onto one or two chips—allowing an entire computer to be built in a small box. The 'Personal Computer' age dawned.

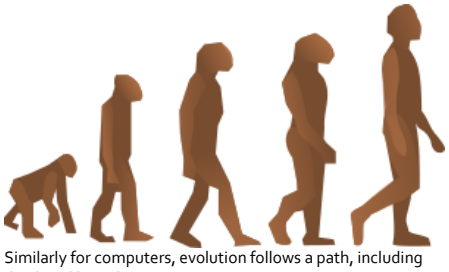
Traditional Datacentre

PCs had their limitations and, after a honeymoon period, the central computer room returned, using racks of servers evolved from the PC.

This permitted the evolution of massive storage, applications, security, etc. and resulted in the need for a host of IT specialties around servers, storage, network, security, etc.

Virtualization

Traditional datacentres grew, sometimes housing thousands of racks of servers, with most servers using a small portion of their available 'horsepower'. Then software was developed to allow servers to be virtualized, with physical servers hosting many virtual servers. Many benefits were achieved including the ability to easily rehost a virtual server if the host server failed.



Similarly for computers, evolution follows a path, including dead-end branches

The Cloud

As communications technology evolved it became realistic to group applications together in more remote centres and simply deliver the application to the desktop from 'The Cloud'. Proponents sang the praises of no longer having to even build an IT infrastructure.

Converged

Data centres, including cloud providers, evolved and improved, but continued to operate with functional silos—separate boxes for servers, storage arrays, backup devices and others. The idea of convergence brought the boxes together into an integrated module containing all the hardware systems needed. Done in a 'plug and play' manner, it was pitched at reducing costs and simplifying design by dealing with modules, not separate boxes. Users added modules as extra capacity was required.

Hyperconverged

Converged modules had limitations similar to physical servers with unused capacity. Not to be out-done, companies that specialised in virtualization realised that they could 'virtualize' the separate hardware components into one hardware module that looked like multiple appliance boxes. The name comes from adding the core of virtualization, the Hypervisor, to converged.

Which is Best?

There is no one 'fits all' right answer. Virtualized datacentres and cloud options continue to work well for many as do converged and hyperconverged designs. As with most things, it's easy to decide when you've established requirements.

This article is reproduced from the April 2017 edition of ***TMC's Advisor***

Ellen Koskinen-Dodgson is President and Managing Partner of TMC IT and Telecom Consulting Inc. She is an IT and Telecommunications Management Consultant, electrical engineer, author, speaker, media resource and Expert Witness.