Clearinghouse for Global Mitigation Best Practices

what are we trying to achieve?

How can we move beyond the “ACK?”

> This document is a worksheet to collect ideas, notes, and other observations needed to fulfill the FCO Explicit Expectations.

Build a select set of Security Hygiene BCPs that can be directly measured using CyberGreen Data. We create materials that can “train the trainer” to be used with National CERT Teams and other teams. The National CERT Teams would then use these materials to work with their constituents. Results would be measured via CybeGreen.

We would use the FIRST 2016 as a tool to test and socialize the materials. This would allow tuning and a validation to understand what CERT Teams are seeing as top priorities.

Execution Details

Collect mitigation best practices for systemic risk conditions (Top BCP Approaches: including Open DNS resolvers, Open NTP, clean up spam bots...) ----> *by the end of July 2016*: deliverable - documents or ppt

Hold workshop in Korea (FIRST conference) collect + validate above with community ----> by the end of June, deliverable: 10< best practices validated by community (ppt or doc)

Develop training materials of above mitigation best practices (ppt slide) ----> training targeting CSIRTs and AS operators ----> by the end of July

Production Principles

Where possible use the BCOP aspirations in the operations community to build the CyberGreen Materials. This build an automatic peer review system with the major operators of the world.

Use Creative Commons for all CyberGreen activities.

what are the "Top" Measurable BCPs?

As an industry, we've been able to teach BCPs. Knowledge of the BCPs are not the challenge. The challenge will be the metrics to see results AND action plans for how to plan and deploy the BCPs within a network. Using BCP metrics on organizations who have not budgeted the planning time, lab testing, operational integration, customer impact testing, and deployment models is equivalent to "pushing rope." The Operator will not move and will often push back if the BCP "ask" is not aligned to their business objectives. The following candidate BCPs are designed to build resiliency into the Operator's network while having measurable impact.

The Short List

The following items will be reviewed at the FIRST Workshop. These

CyberGreen Methodology - Publicly Visible Security Hygiene/Mitigation/Remediation Metrics that Facilitates Action. The Community has a wide range of data sets that provide list of systems used in attacks, infected with malware, and vulnerable to attack. There has been several informal community lead, vendor lead, organizational lead, and collective action lead activities to use this data to remediate the risk (remediation is in this case is the reconfiguration of the risk, removal of the malware, or patching the vulnerable system). What we're missing is are systematic approaches to improving the security hygiene of the Internet. The CyberGreen Methodology will explore these approached, build measurements to gauge their impact, and then facilitate the implementation to understand their effectiveness. Measureable Action with Repeatable Results is a core theme.

Systematic Problem Solving. As CyberGreen's methodology evolves, unforeseen dependencies will be uncovered new problems which will then need to be solved. For example, as CyberGreen evolved an incident notification process and the CERT Teams are able to craft a constituent notification system, these same constituents will struggle with tools with their organization to take action. If the CERT constituents are not able to remediate, then a barrier to improving the metrics emerges. A role of CyberGreen would be to use the data driven methodology to find these coupled dependencies. Other groups can be partnered to work to clear the path with new tools. The value of CyberGreen's methodology would be the measurement - as the new constituent tools are applied, measurements can be used to understand their effectiveness.

DNS Open Reflectors - Has several active scanning activities with data that can be used to build a remediation tempo with measurable impact. The benefit would reduce the industry risk exposure and the impacted ASN's specific risk exposure.

NTP Open Reflectors - As with DNS Open Reflectors, NTP has an active scanning activity that can easily be integrated a tempo of remediation operation.

General UDP Reflectors - While DNS and NTP are the two most popular UDP based reflectors use for DDOS, they are not the only ones. Other protocols like SNMPv2, NetBIOS, SSDP, CharGEN, QOTD, BitTorrent, Kad, Quake Network Protocol, Steam Protocol RIPv1. Multicast DNS (mDNS), Portmap/RPC and several other protocols can be used as UDP DDOS reflectors. Each of these can be include in CyberGreen data sets, mitigation actions crafted, and remediation efforts explored encourage the deployment of these actions.

Measuring Spoofing Capabilities. The Spoofer Project (https://www.caida.org/projects/spoofer/) will team with key community partners. Given this, CyberGreen will team with the Spoofer Project to teach constituents how to deploy the spoof sensors, how to use the data, and how to then build mitigation and remediation best practices. Each ASN would need to build their "BCP 38" plan of action.

Malware Remediation Exercises. Malware systems that have been sinkholed or taken over allow the community drive an industry infection to zero. These violated systems are an double risk from the known infector and the additional infections that are likely given that most malware disables updates and security software. Several groups in the community have agreed to work with CyberGreen to use their data along with the specific Clearinghouse training.

Vulnerability Remediation Exercises. Vulnerabilities are persistent attribute of our hyper-connected world. Given this, the time between an announce vulnerability and exploitation is small and often is driven by the perceived derived value of the exploitation. For example, a vulnerability that can be turned into direct criminal revenue potential has a high chance of a short "gap" between the vulnerability disclosure and the first active exploit. What CERT Teams need are approached to rapidly obtain measurable data on the vulnerability risk with their constituents, build metrics to measure that risk, and then drive mitigation/remediation techniques to reduce the risk.

The Security Toolkit Approach. There is not one "security tool" that can cover all security issues encountered by an Organization. The "Security Toolkit" approach uses a broad set of security capabilities. Each security capability has a an impact and appropriate use. The Clearing House materials teaches several of tools for the security toolkit in a way that adds capability to the team. In addition, the teaching methodology is crafted to inspired the team to look at all technological functions as potential "security tools." This open point of view builds capacity in

the team to be open to out of the box ideas to how technology can be used to mitigate and remediate security issues.

Data Sources and Managing those Data Sources. There are more security data sources that people realize. As part of CyberGreen Phase 1, there was a concerted exploration on how the CyberGreen data partners can be highlighted and relationships would be enhanced. Going forward, this "CyberGreen partnership" enhancement would move forward. It would focus empowerment materials to share with the team the data contributed into CyberGreen and how each CERT Team would be able to build their own 1:1 relationship with that security data partner.

Building the Telemetry Capabilities within the CERT Constituents. One element of building security data partner relationships is through the expansion of the sensors and data collection efforts. CERT Teams would be taught several examples, how they could encourage their constituents to participate, and then how that benefits all of the CERT's constituents.

What Can Be Measured?

We have four major area that allow effective data collection: Open Exploitable ports, Malware infections, vulnerabilities accessible via the Internet, and BCP violations.

Open Exploitable Ports

Open Exploitable Ports are considered to be services that are needed on the Internet, but have risk which allow these services to be used unexpectedly to cause disruption on other parts of the Internet. DNS Resolver Reflection is the most famous these classes of open exploitable ports. We can scan for these ports, test their "exploitability," and then apply metrics to this data. DNS Open Resolvers and HeartBleed are two examples. Each can be consistently scanned over time and used to metric the effectiveness of remediation actions.

Malware Infections

The battle with malware builds data sets of the specific elements who are infected. While there are many ways of collecting this data, the most accessible malware infection data sets are from sinkhole take downs. The Community builds view of the malware system and then deploys tools which intercept the malware command and control (C&C) telemetry. This would then provide a

list of devices on the Internet which are infected by this specific malware. Conficker and DNS Changer are two examples from this class of activity.

One key limitation with the C&C approach will be the Operator's ability to convert a PAT/NAT data point from the sinkhole report into a trackable element inside the Operator. If PAT/NAT logs are kept by the Operator, these logs will be time limited, with the key data often overwritten days after the receipt of a malware infection report. The speed in which the malware infection report reaches an Operator is critical.

Malware Mitigation & Disruption → YES, partially. The picture is never 100% complete, but yes, we can

Malware Remediation → YES, for every ASN_j we calculate

$$remediationRate_{ASN_j} = (\sum_{i=0}^{N} a_i(\Delta\, numInfections_{risk_i})) / activeIP\,space_{ANS_j}$$

Where:

$\Delta\, numInfections_{risk_i}$ = the change in number of infections we see in this particular IP space since the last measurement for the i^{th} risk we assess.

$activeIP\,space = average(numActiveIPs)$ over a time window. An IP is active if there is some kind of indication that it does have traffic to-from it (some netflows) which indicate some reaction from this IP address (i.e. network telescopes don't count)

a_i is a weight factor for the i^{th} risk we assess.

Examples from the past where the people driving the malware became exhausted.

Vulnerabilities Accessible via the Internet

Some classes of vulnerabilities are remotely exploitable. The Common Vulnerability Scoring System (CVSS), would be a Network Attack Vector defined as:

> *A vulnerability exploitable with network access means the vulnerable component is bound to the network stack and the attacker's path is through OSI layer 3 (the network layer). Such a vulnerability is often termed "remotely exploitable" and can be thought of as an attack being exploitable one or more network hops away (e.g. across layer 3 boundaries from routers). An example of a network attack is an attacker causing a denial of service (DoS) by sending a specially crafted TCP packet from across the public Internet (e.g. CVE 2004 0230).*[1]

[1] See Common Vulnerability Scoring System v3.0: Specification Document - https://www.first.org/cvss/specification-document

These classes of vulnerabilities might have characteristics which are measurable through external scanning. If this is the case, they would be measurement candidate. This would only work if the vulnerability can be scanned with no collateral consequence. For example, scanning for the 2002 SNMP Protos vulnerability would triggering the vulnerably.

BCP Violations

Best Common Practices (BCPs) are highly recommended. There is an assumption that BCPs are widely deployed. Yet, the data from attacks demonstrate that many ASNs have not deployed key BCPs. This creates a situation where measurable analysis might be use to motivate action. The question is how to determine how the BCPs can be measured.

Some BCPs can be measure from outside monitoring of scanning. For example, port scanning data of a ASN could be parsed to determine network element's management and control plane ports. The minimal BCPs would be to protect these ports from access outside the ASN. Hence, data like this can determine and ASN is protecting their network using Infrastructure ACLs and other BCPs techniques to add safeguards to the Management/Control Plane.

Spoofing harder, how would you without the ISPs' cooperation?

Protocols That Should not be Exposed

There are protocols that are commonly exposed to the Internet. The vast majority of organizations do not run external to internal scans to check their network for these protocol exposures. While there are many commercial services that run external to internal scans, there are also a multitude of security data sources with some of this information. One approach would be to have a CERT team take one of these open protocol vectors, build a measurement tool of the numbers impacted in an ASN, then use the notification to encourage a check on all their ports.

what Cannot Be Measured?

Essential Monitoring (Scan Rate Monitoring)

Breaking the New Habits into Small Parts - Using Incidents as a Tool to Explore Changing Behaviors

One observation of CyberGreen's phase 1 is the intimidation of the problem. A National CERT team exploring plans of action can easily be overwhelmed with the volume of data available to take measurable action. In many ways the volume and depth of the problem would make it seem that any small level of success would fail to demonstrate measurable success. Given this, one approach that will be used during the Clearing House Workshops is to use specific incidents as a tool for success.

For example, an Operator works a DDOS attack on their customer, pushing back against a DNS Reflection based attack. The Operator is able to collect over 200 DNS Open Resolver addresses. CyberGreen works with the Operator to take this list of 200, break into the ASNs (Team CYMRU Tool), and then work with each of the CyberGreen CERT constituents to remediate the problem. CyberGreen can publicly express the over all "incident remediation progress" by anonymizing the specific host, but maintaining a "risk count" for each ASN.

Success is declared by driving the list from 200 to 0. The CERT Teams and CyberGreen learns valuable lessons each time an incident remediation reaches a conclusion. The key is to find the tools to communicate to the ASNs and organization below the ASNs in a way the motivates action.

Capacity Building what will need to be Taught?

New generations of cyber-security professionals do not have the essential knowledge, skills, and capabilities need to participate in an industry wide mitigation/remediation incident. We cannot assume the skill are present.

Example: While conducting a workshop of a "1st world" national CERT Team, none of the key people realized the role of BGP and DNS as critical security tools to mitigate DDOS Attacks. Assuming they have an understanding of these fundamentals is a mistake. Taking the time to teach these fundamentals will be key.

What is out of Scope for the Round?

Time Table

2016

April : mitigation capacity building Material development (outsource : Barry? how much?)
Metrics training material --> who build this? stats group?

May: v.2 Metrics development ongoing

June: FIRST 2016, in South Korea. (Candidates AfriNOG AfricaCERT training at Botswan)

July: (RSA Side Event in Singapore with SGCERT and CSA?)

August : India and South Asia NOG meeting

September : Latin America NOG at Costa Rica

October : APCERT / OIC-CERT in Tokyo

November :

December :

Jan : SANOG pakistan

Feb :

March :

Other meeting to go together -- for policy makers
- APEC-TEL, ITU, GSMA..... etc

FCO Explicit Expectations

Output
- 1. Work with national CERTs and experts to collect best practices to mitigate risk conditions, and develop Mitigation practice guide (training material)
→ YES

- 2. Measure efficiency of each best practices (with green metrics / feedback from operators)
→ YES, question: how to stay in touch with network operators through cybergreen? How to push their new metric/status to them?

Milestones:
- Semi-annual update of best practice guide validated and ranked for effectiveness
→ YES

Target and dates:
- Technical Validation workshop held June (at FIRST)
- Best Practices Guide v2 available July 2016

provide metrics, mitigation best practice gathering and capacity building tour.

Definitions, Terms, Concepts, & Principles

The following is a list of terminology used within the CyberGreen participants. It is provided here to help readers understand concepts, terms, and principles which are just "assumed" to be essential knowledge.

- **The Community.** The "white hat" operational community is several thousand professionals who work within trust groups to battle the threats, risk, and security challenges we face on today's hyber-connected world. We will refer to this collection of white hat individuals as the Community.