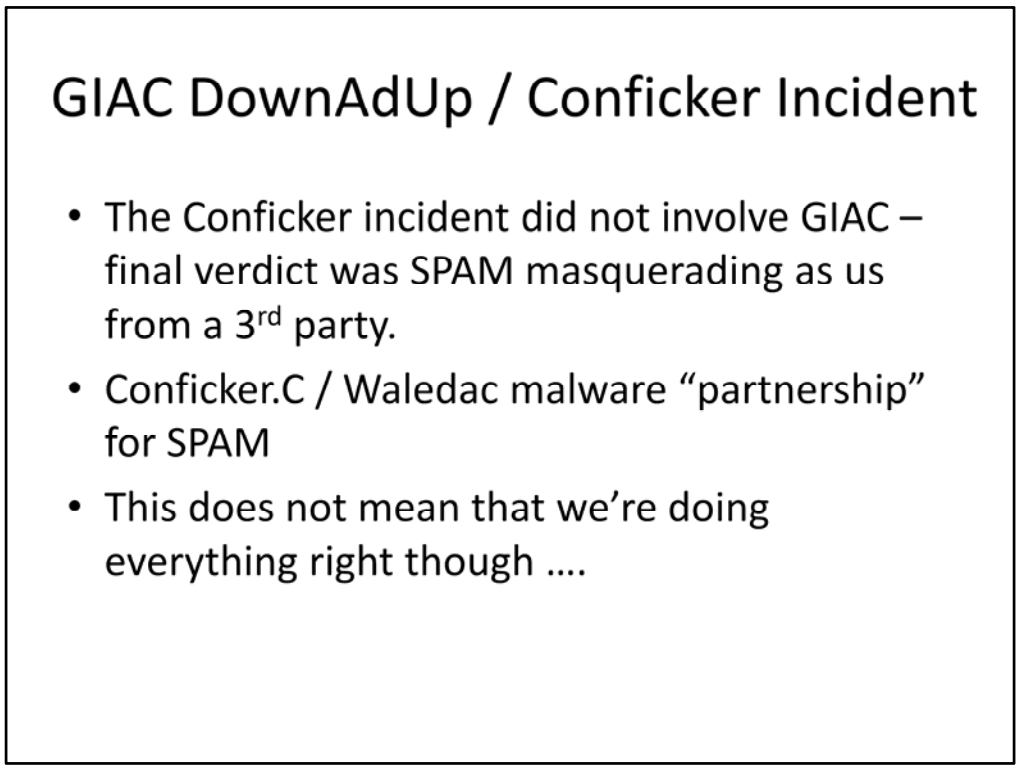


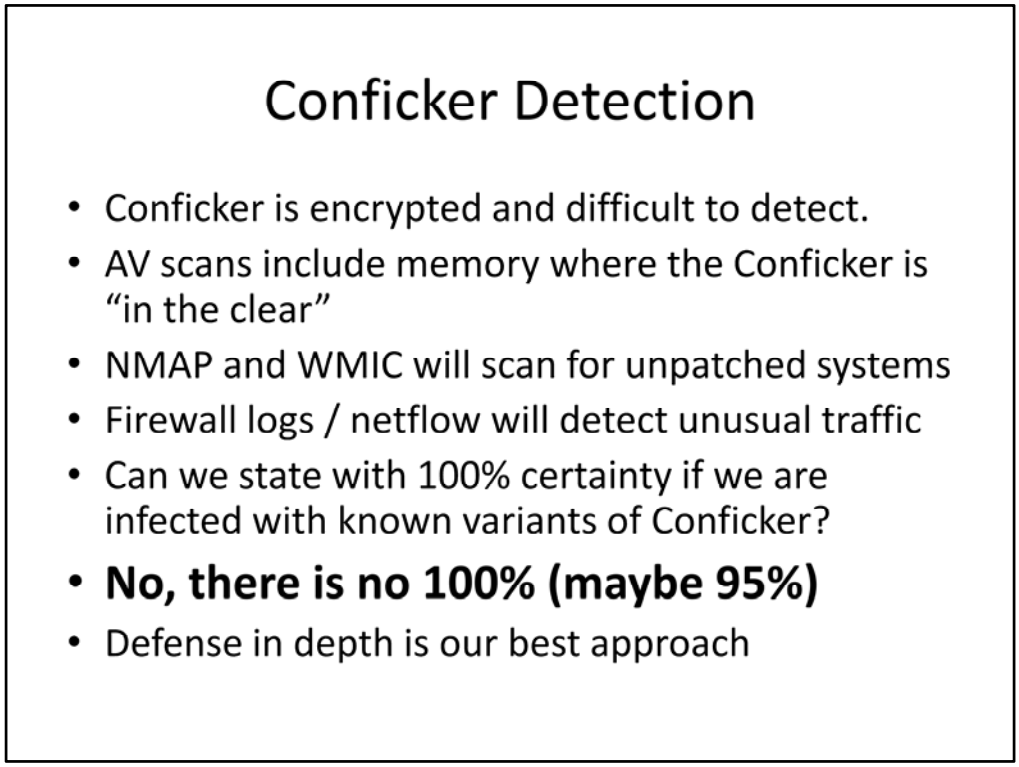
The conclusion we reached is that the recent event probably involved an DownAdUp infection, but not at GIAC. It was most likely a spam email sent from the companion virus Waledac, which "piggybacks" on DownAdUp.C and newer variants. The initial email probably originated from outside of GIAC, and was simply masquerading as a email from the GIAC CIO. We would need the email server logs from the target organization to comment any further on this.

However, the exploration into the incident has brought to light several related issues at GIAC that should be dealt with. The concern for the DownAdUp virus should be extended to the thousands of other malware packages that are created each day, and some basic changes to our IT infrastructure and team should be considered. These are separated into recommendations of low or no cost, and recommendations that should be considered for next years budget. First, let's consider the low/no cost recommendations:

What does Conficker do?

- No-one knows what it was originally intended for
- Primarily it spreads, using open shares, weak passwords, missing patches (MS08-067 / KB958644)
- "Phones home" for updates
- Many variants, lots of payloads and attack vectors
- "Phones home" for botnet instructions, this has not yet happened
- The act of spreading impacts IT infrastructure

Variant	Spreads Via...	Payload	Additional Information
Worm:Win32/Conficker.A **Discovered Date:** 21st Nov 2008 **Payload Trigger Date:** 25 Nov 2008 and later	-Exploiting the vulnerability outlined in Security Bulletin MS08-067.	-Generates 250 URLs daily that it checks for updates -Resets System Restore Point	The name of this family was derived by selecting fragments from 'trafficconverter.biz', a string found in this variant.
Worm:Win32/Conficker.B **Discovered Date:** 29th Dec 2008 **Payload Trigger Date:** 1 January 2009 and later	In addition to the method used by the .A variant (above): -Network shares with weak passwords -Mapped and Removable drives -Uses a scheduled task to execute copies of the worm on targeted machines	In addition to the .A variant's Payload (above - although .B uses a different method to generate URLs): - Blocks access to many security-related websites -Modifies system settings -Terminates system and security services	This variant built on the functionality of the .A variant by adding new spreading mechanisms and by making itself more difficult to remove.
Worm:Win32/Conficker.C **Discovered Date:** 20th Feb 2009 **Payload Trigger Date:** 1 January 2009 and later	Uses the same methods listed above for the .B variant.	In addition to the Payloads listed above for .A and .B: - Uses additional method for downloading files that utilizes Peer-to-Peer communications - Adds checks to verify the authenticity/validity of content targeted for download	Very similar to the .B variant in function (this variant has even been referred to as variant .B++).
Worm:Win32/Conficker.D **Discovered Date:** 4th Mar 2009 **Payload Trigger Date:** 1st April 2009 and later	No spreading functionality per se. Distributed as an update to machines previously infected with the .B and .C variants.	In addition to the Payloads listed above for .A and .B, with some variations: - Generates 50,000 URLs to download files from. This variant only visits 500 of the generated URLs within a 24-hour period. - Expands on efforts to hinder its removal from an affected machine.	Spreading functionality was removed from this variant. It continues to expand on its file downloading payload and targets a broader range of processes to terminate (appears to be targeting cleaning utilities designed specifically to remove Conficker). It also blocks access to additional security-related websites.
Worm:Win32/Conficker.E **Discovered Date:** 8th Apr 2009 **Payload Trigger Date:** 1st April 2009 and later	No spreading functionality per se. Utilized to update machines previously infected with the .B and .C and .D variants.	- Blocks access to many security-related websites -Modifies system settings -Terminates system and security services -Terminates itself on May 3	May have been distributed via the Conficker peer-to-peer network.



Scanning for patched or vulnerable systems can be done in a few different ways:

NMAP:

```
nmap -p139,445 -n -v --script=smb-check-vulns --script-args safe=1
192.168.10.0/24
```

WMIC:

```
wmic qfe where hotfixid="KB958644" list full /node:%1
/user:<domain\administrator> /password:<domainadminpassword>
```

These scripts are expanded to full solutions in the paper to include scanning entire subnets, or scanning an entire AD Domain

Recommendation - Detection of other Zero Days

- A/V signature approaches cannot detect "zero day" infections
- Integration of firewalls makes A/V tools better
- Zero Day Detection Recommendations:
  - Monitor firewall netflow and logs
  - Scan the network frequently for new open ports
  - Scan desktops and servers for new processes

Example Netflow display to detect anomalous traffic:

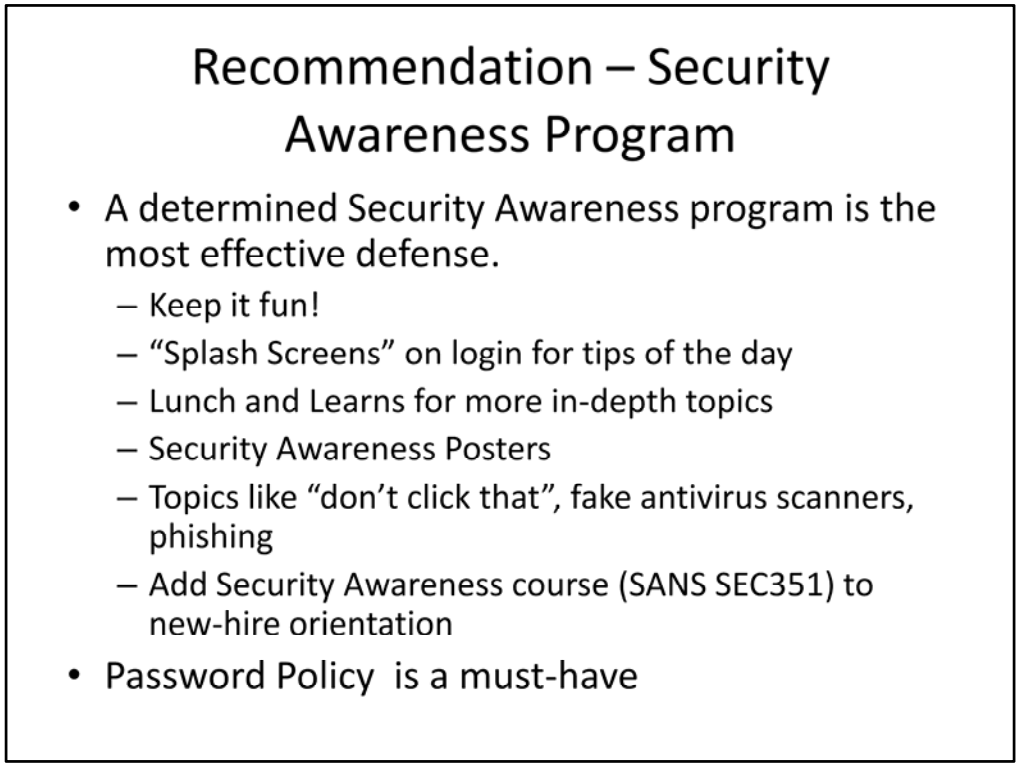
Scanning the network for new open ports

```
nmap -sT  192.168.10.0/24
```

Scanning stations for running processes

```
wmic process list brief /node:%1 /user:<domain\administrator>
/password:<domainadminpassword> | /format:csv | cut -d, -f
1,3
```

Again, these scan approaches are expanded to more complete solutions in the paper, to scan complete subnets or AD Domains.



Security Awareness training is the most critical area we should focus on to reduce the malware infection rate at GIAC Enterprises. Training can be done in dedicated sessions, or in more informal settings. For instance, attending SANS SEC351 (which we are certified to present) would be a good option for our new-hire orientation program. Alternatively, we could create our own training course based on NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program.". For a more immediate benefit, however, we need to target our existing employees, and a mandatory 3 hour class is probably not an effective way to do this quickly.

Malware, and Conficker in particular, will take advantage of blank passwords, open shares, and simple passwords. Conficker in particular in some variants had a process to brute-force passwords. For this reason it's important that as a corporation that GIAC creates a Password Policy outlining clear policies on password strength and frequency of password changes, with non-technical guidance for our users in plain language. We then need to communicate these policies to our user community, and follow this communication up with periodic audits and assessments of domain and local credentials. Our password strength policy should then be implemented as a Group Policy within Active Directory, to ensure that our users comply going forward. As we ramp up this policy, frequent might be advisable. Once the policy is in place, tapering down to monthly or bi-montly assessments should be sufficient.

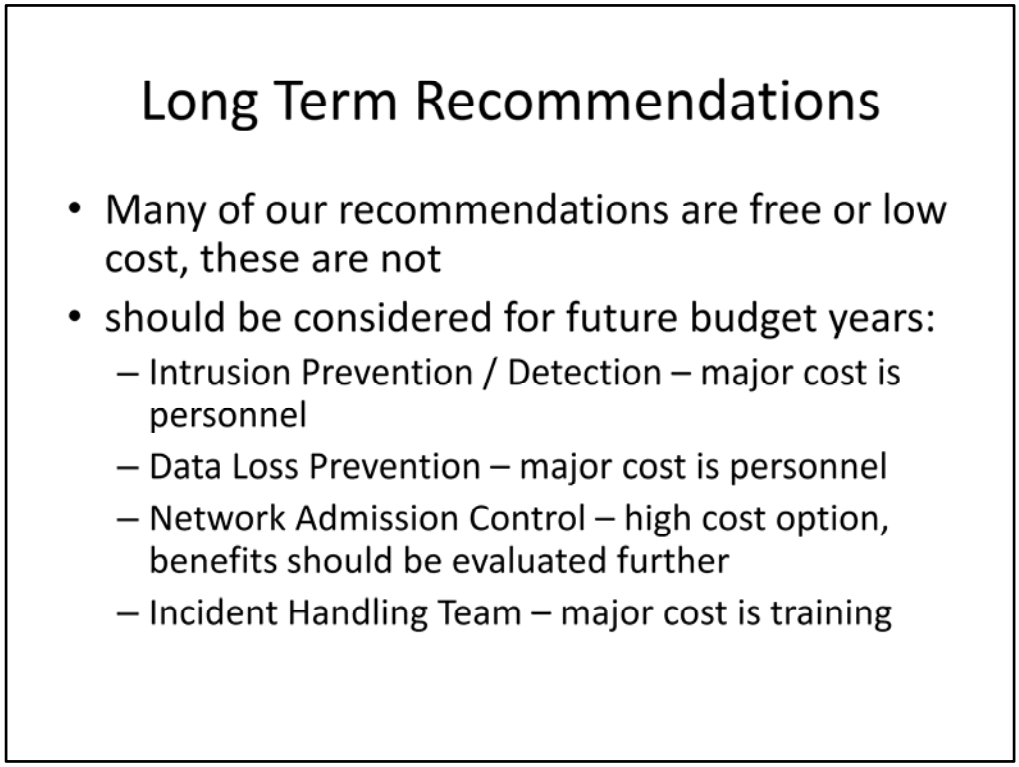
Recommendation – Patching and A/V

- A new trend is short-lived malware (<24hrs)
- However, a layered defense is still our best technical option
- Target applying patches within 24 hours
- Only ~29% AV detection in first 24 hrs of malware release
- Look at different AV vendors for mail, web and desktops – Layered Defense

Patching:
WSUS is a free Microsoft approach to patching it's operating systems and applications, and could be used effectively at GIAC. If, after study, we decide that other business applications need to be patched in a similar way, we can expand our WSUS deployment with custom scripting, or we could migrate to a commercial product such as Altiris Total Management Suite or GFI Languard.

Malware:
Of the 37,000 new samples of viruses, worms and trojans that anti-virus firm Panda Security receives daily, 52 percent spread for just 24 hours. Nineteen percent last for two days, and nine percent persist for three days.

A reasonable approach for GIAC to take to mitigate this new trend is to layer our malware defenses. We might take a 3 vendor approach, with different AV solutions for our mail filtering, web filtering and workstation AV engines. This will however mean that we'll also have 3 different management consoles and 3 different reporting solutions for malware.



We would be remiss if we did not mention these additional recommendations. While they are outside of our mandate of not impacting the IT budget, we feel strongly that these items should be considered as projects and ongoing line items for upcoming budgets:

Intrusion Prevention collects all data on the network, generally at significant points (DMZs, ingress and egress points for example), then reassembles the collected data into complete streams. This is then compared to the behavior or signatures of known attacks. If an attack is detected, it can either be treated as an alarm and/or alert, or the IPS can block the datastream.

Data Loss prevention, at least in the context of the network data leakage we'll be concerned about from malware, is all about categorizing and recognizing data on the wire. In our case, we would be categorizing our customer information, and of course our Fortune Cookie Sayings, our main intellectual property. In both cases, our DLP system would need to know where this data was *not* allowed to travel.

Intrusion Prevention, Intrusion Detection or Data Loss Prevention would all require an Incident Handling Team in order to function correctly.

NAC (Network Admission Control), or the Microsoft NAP (Network Access Protection) can both be used to enforce a defined security policy on our entire workstation population, including visitors. Both approaches act as GUI interfaces and database back-ends to the 802.1x protocol implemented on modern switches.

Something that we allude to in both solution descriptions is an **Incident Handling (IH)** team, something which does not currently exist at GIAC. Creation of an Incident Handling team will also carry some costs, not so much in dedicated resources , but in initial and ongoing training. It's important that we not only train our team members and define a methodology for handling incidents (SANS Security 504 would be an ideal choice for both), but will need to participate in regular Incident Handling exercises and ongoing training.