WELL, WHAT HAD HAPPENED WAS
whoami

- Hello, my name is Todd Mesick
- Worked in IT since 2000
- Switched to primary security focus 2013
- Full time IR in 2014
- Champlain MS grad 2017

Full time student of infosec, and been blessed to make some of the best contact, and great mentors
  - Recently became an adjunct to help give back
Hello, my name is Brian Moran
13+ years Air Force career
   – 16ish years mobile exploitation/DFIR focus

Started BriMor Labs back in 2014, have been very happy since!
Ladies and gentlemen: the story you are about to hear is true. Only the names have been changed to protect the innocent.
Well, what had happened was...

- Got a call from Callahan Auto Parts that they had an issue
  - Tuesday AM received the popular (dreaded) 3 letter agency call
  - Initial IR started and first round of machines identified
  - Live Response was run and overnighted to myself (Todd) and driven to BriMor Labs to review

- In addition, call was placed to Zalinsky Auto Parts team for product line
  - They claimed they were familiar with the attacker and offered assistance
Well, what had happened was...

- First review of IOC (a whopping 2 external IPs) identified four systems of interest
  - The “first four” and some serious digging yielded the systems to survey
- Advised to perform a typical incident response process
  - Run the Live Response Collection (LRC) on affected machines
  - Overnight the collected data to me (Brian)
Well, what had happened was...

- Data gathered by LRC showed probable compromise with questionable entries in:
  - Startup folder
  - Persistence mechanisms (from LRC output)
  - Modified “hosts” file (Windows\System32\drivers\etc\hosts)
  - DNS cache anomalies

- Recommended consultant on-site to client location
Well, what had happened was...

• Made initial contact with members of government agency (on a personal level) to inform them I had some interesting indicators to share

• Advised to share indicators informally via SneakerNet, as an external information sharing process was not set up
I’ll Take “NOLA Notable” for $350

- **NOLA NOTABLE**: It is now the year 2019, and there *still* is no formal external information sharing process in place. Don’t let a lack of formal process dissuade you from doing what is “right”
IMPORTANT ITEMS TO NOTE

• Up until this point, everything that was done cost the client ZERO dollars
  – With the exception of hard drive for LRC data & shipping

• BriMor Labs Live Response Collection - Cedarpelta
IMPORTANT ITEMS TO NOTE

• This means any sized business can take these steps
  – You don’t need a massive SOC or IR team
    • Trust me, we didn’t have one!
  – You don’t need a multibillion dollar security budget
I’ll Take “NOLA Notable” for $350

• **NOLA NOTABLE:** You need to know the right people and companies to engage with BEFORE something bad happens
  – This is a common theme throughout the cyber security industry
Flying to client site
On-site at last

- By this point, we have a few basic IOCs from a variety of sources:
  - Customer company that was interested in helping
  - Some from online research (OSINT)
  - Some from personal contacts (DC3, other IR companies, other companies)
  - Lastly the 2 external IPs provided by the original call.
How (most) clients view consultants entering client site ...
How (most) consultants view themselves entering client site ...
On-site at last (T PLUS 4 hours)

• Identified approximately 20 new, never-before-seen IOCs & shared with:
  – Govt. orgs and other IR companies (including competing companies)
  – Customer who initially offered IOCs/assistance
    • At this point, contact with Zalinsky Auto Parts stopped
      – “Sir, there could be some merit in NOT discussing that”
I’ll Take “NOLA Notable” for $350

• **NOLA NOTABLE:** Always keep open communication with IOC sharing entities. It takes a village, and sometimes the villagers work for more than one employer
On-site at last (T PLUS 16 hours)

• Identified domains related to C2 connections
  – Reached out to individual employed by company who controlled C2 domains
  • Within an hour, ALL C2 domains were down (including other domains they associated with this threat actor)
- From a consumer of IR services, this was huge for us
I’ll Take “NOLA Notable” for $350

• **NOLA NOTABLE**: A simple contact here made the major bleed stop. Sometimes all it takes is knowing the right person, or knowing the right person to reach out to for help.
On-site at last (T PLUS 16 hours)

• BONUS: Informally shared back additional IOCs to look for
On-site at last (T PLUS 40 hours)

- Identified/remediated all systems initially compromised
- Continued monitoring of environment for additional activity
- Initial remediation was timed to coincide with previously scheduled down time
  - When network came back up, remediated machines did not

- Decision was made to return home & continue analysis remotely
It’s Not a Bug, It’s a Feature

• Attackers utilized a folder that was used on a previous DFIR engagement as a staging ground for their malware

• Folder was white-listed from every single security application, including the security application itself!
Think we all agree this is bad....
Yup, this is bad....
I’ll Take “NOLA Notable” for $350

- **NOLA NOTABLE**: Ensure that ANY application and/or security system is configured for YOUR environment. Regularly clean up old/unused applications & security policy exceptions
On-site Part II

• Remote analysis occurred for ~ 3 weeks
  – Forensic analysis uncovered additional forms of malware to accomplish additional goals
  – Client noticed additional unexplainable activity
    • This was all identified on the network side, using indicators from each resource

• Decision was made to return to client site
On-site Part II

- Additional machines were discovered as being compromised
- Also account credentials were compromised and being used
- Analysis revealed attacker utilized a _VERY_ sophisticated form of persistence
On-site Part II

• Attackers persisted on server by using DLL load order hijacking
  – WMI was set to automatically run (not standard) on boot and malicious DLL was loaded by WMI process
• Yes, you read that right. They used WMI **ITSELF** for persistence. Not the typical “used WMI to create a persistence mechanism”
  – System also had China Chopper on some web-facing pages, including one page created entirely by attackers
• This allowed us to share definitive IP addresses & locations
Attacker mistakes FTW!

- Web traffic to the attacker created web page only occurred when attackers accessed it
  - No one else knew about the page
- Many IP addresses, from all over the world, were logged as accessing this webpage
- Fortunately, all it takes is one mistake!
  *(In this case, the same mistake was made 7 different times!)*
This is what we call a “clue”

*Handmade “pew pew” map*
On-site Part II

• Malware was on critical operational server that could not be taken offline
• Had to come up with plan to remediate malware with absolute minimal down time (~3 minute window of down time was all that could be allowed)
  – So, in other words, no pressure!
• After some thought, came up with solution get rid of malware/webshells & keep the system running until it could be reimaged & restored to 100% clean state
Incident Summaries

• Assembled team of ~ 5 individuals spent about 350 total hours per person to remediate the issue
• Uncovered at least four “generations” of malware as attackers attempted to expand compromise foothold
• Saw combinations of traditional malware/tactics, targeted malware, web based compromises, web shells, etc.
Taking the Next Steps

• Client was happy to share Indicators of Compromise with every entity possible
  – “We saw this as a way of protecting our business vertical as a whole”

• The needs of the many outweigh the needs of the few

• Because of personal relationships, several “abnormal” things happened
Taking the Next Steps

• Online infrastructure used by the attackers were taken down very quickly
  – Entity could not share information directly, but could advise to “look at this/look at that” to piece together additional IOCs
  – IOCs allowed client to better protect all users & identify future attempts
Taking the Next Steps

• US Government agency got approximately 50 pieces of malware associated with threat actor group they would have never received otherwise
  – Information was shared with all gov. agency partners
Taking the Next Steps

• Not limited to a single source, additional information provided by additional collaborators, open source research, etc.
  • IOCs also shared with government office responsible for the management of personnel, who subsequently “discovered” a data breach

• Didn’t matter if attackers were in initial attack phase or last ditch persistence attempt, we had the entire attack life cycle of malware/IOCs
It’s just a jump to the left ...
Time Warp. Destination: 2018

- In October 2018, first indictments issued in case
  - Gained insight to entire investigation
  - Finally was able to piece together entire scope of the attack
Who

• Attackers were from the Jiangsu Province Ministry of State Security (MSS)
  – This is a “provincial foreign arm” of the MSS

• This group included:
  – Six agents
  – Two Chinese national insiders (Worked for supplier)
What

• Attack focused on thirteen companies in total
  – Companies were all in the supply chain of the target product
  – Target product owners first to be compromised, by insiders in Chinese facility
What (cont.)

- Yes, you read that right. A multi-faceted attack that included actual insider threats!
- Human Intelligence attempts occurred by meeting engineers
- Incredible amount of resources/money and energy went into this operation
Where

- Targeted companies were mostly US or UK based
- Human Intelligence sources believed to meet in EU. Engineers thought they were meeting potential colleagues from the foreign power. Undetected until one reported

- Only serious international targeting was at the product owners facility in China
  - This seriously complicated the overall response process as insiders fed investigation data to the attackers
When

- First attack (outside of the insiders) started January 2010
- Attacks ran until about May 2015
- Many of the companies were attacked around same time - very coordinated
- Human Intelligence operations started late 2014 as compromised companies mitigated network intrusions

A successful IOC sharing medium would of be a HUGE help!
Why

- Attackers were after a very specific product line
- Goal was to build a comparable product to compete
  - Mostly obtained the past twelve months (2018-2019)
How

• Attack started with obtaining insider participation & old fashioned intel/spying techniques
• Insiders inserted a USB device for the attackers kicking off the event
How (cont.)

• Numerous techniques used on rest of the companies

• Waterholes, phishing and all the traditional techniques employed
We ALL Should Be Better

• ANYONE can share information with others

• Especially companies/individuals who, at the end of the day, just want to do the right thing (like the awesome people giving this presentation)

• Personal relationships are SO important! No rules were broken & didn’t do anything “wrong”
We ALL Should Be Better

• Inform company/organizational leadership of benefits of information sharing
  – It is not taboo
  – Help them understand its OK, to “help” competition
  – Help them over the “legal” concerns
• Information sharing can help prevent the same attacks from occurring in different environments
  – This can help an entire business vertical Win/Win
We ALL Should Be Better

• Put your personal feelings/personal goals aside
  – It does not matter how good you think you are, how smart you think you are, how big you are, how small you are, how much money your company makes, what your security budget is, etc.
  – Every piece of information has value!
We ALL Should Be Better

• Our adversaries share information all the time, why can’t we?
  – This is not limited sharing information between companies
  – Information/communication should be shared between Internal red teams, blue teams, purple teams, etc.
I’ll Take “NOLA Notable” for $350

• **NOLA NOTABLE**: Your org should either have an internal red team or engage with a company offering red team services. Otherwise adversaries in China, Russia, North Korea, Iran, etc. will gladly act as your red team for free!

(PRO TIP: You do NOT WANT this to happen)
We ALL Should Be Better

The IR team finding a "five any" firewall rule while responding to an intrusion

Original video credit: @DanyelxDragon
PLEASE Remember This
If Nothing Else

Keeper of Lore
@munin

When you hire an infosec person, you hire their social network as well.

That may be to your -extreme- benefit.

da_667 @da_667
pays to have good contacts.
Questions?

Todd Mesick
Twitter: @tmesick1
Email: tmesick@gmail.com

Brian Moran
Twitter: @brianjmoran
Email: brian@brimorlabs.com