NGS

SECURITY FREEDOM

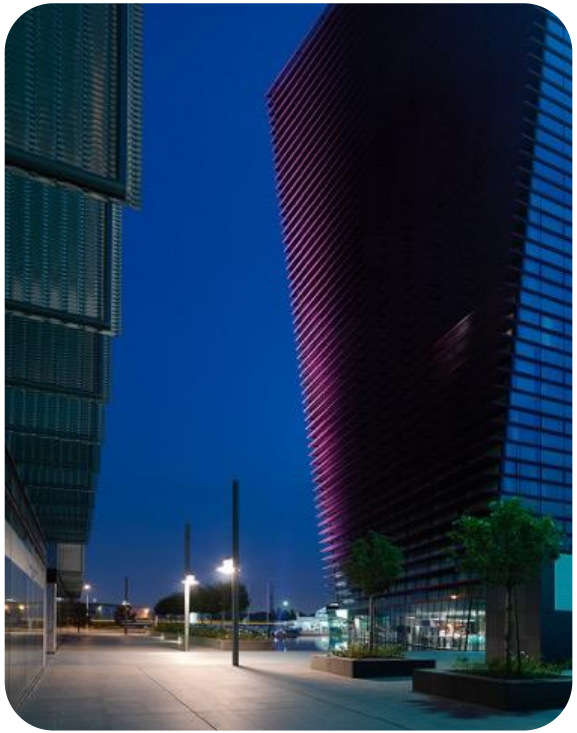
PoC Cyber Range Platform
22/09/2020

About us

We are a **consulting** company specialised in **Cybersecurity,** on the market **since 2012**

We provide innovative and highly-qualified **professional services**

We implement next-generation **information technology infrastructures**, we focus on **IT/OT security**, **system integration** and **automation**. We are **ISO 9001:2015** certified for the quality of our **Services**



Vision, Mission and Values

V Make technologies an enabling factor for Digital Transformation and a driver for business

M Be the Partner of reference for our Customers on information security and innovation issues

V We believe in Innovation and the Value of People, putting the Customer at the centre of our activity.

Why NGS

We work together with our customers in a transparent and responsible manner

We provide significant design, configuration and service **expertise** with highly qualified and certified personnel

We implement **bespoke information technology infrastructures** according to Customer needs

We integrate the most innovative **technologies**

Focussed

- Professional and managed services
- IT/OT security
- Systems integration
- Automation

The method:

- Holistic approach to security
- Customer training

Cyberbit Cyber Range

Introduction

CYBERBIT
TRAIN FOR REAL

About Cyberbit

Who is Cyberbit?

Leading Global Provider of Cyber Range Platforms to:

Upskill Cybersecurity Employees

Assess Cybersecurity Skillset

Optimize Incident Response Playbooks

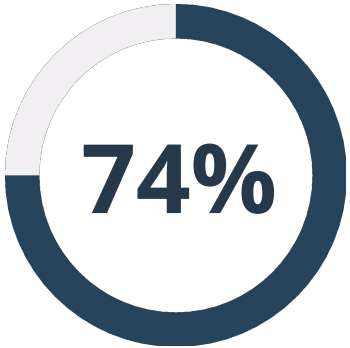
- Live Since 2009
- 150 Employees Across US, Europe, & Asia
- Raised $100 Million+ Since 2016

Charlesbank

CLARIDGE

Elbit Systems™

Cybersecurity Skills Shortage Having a Major Impact



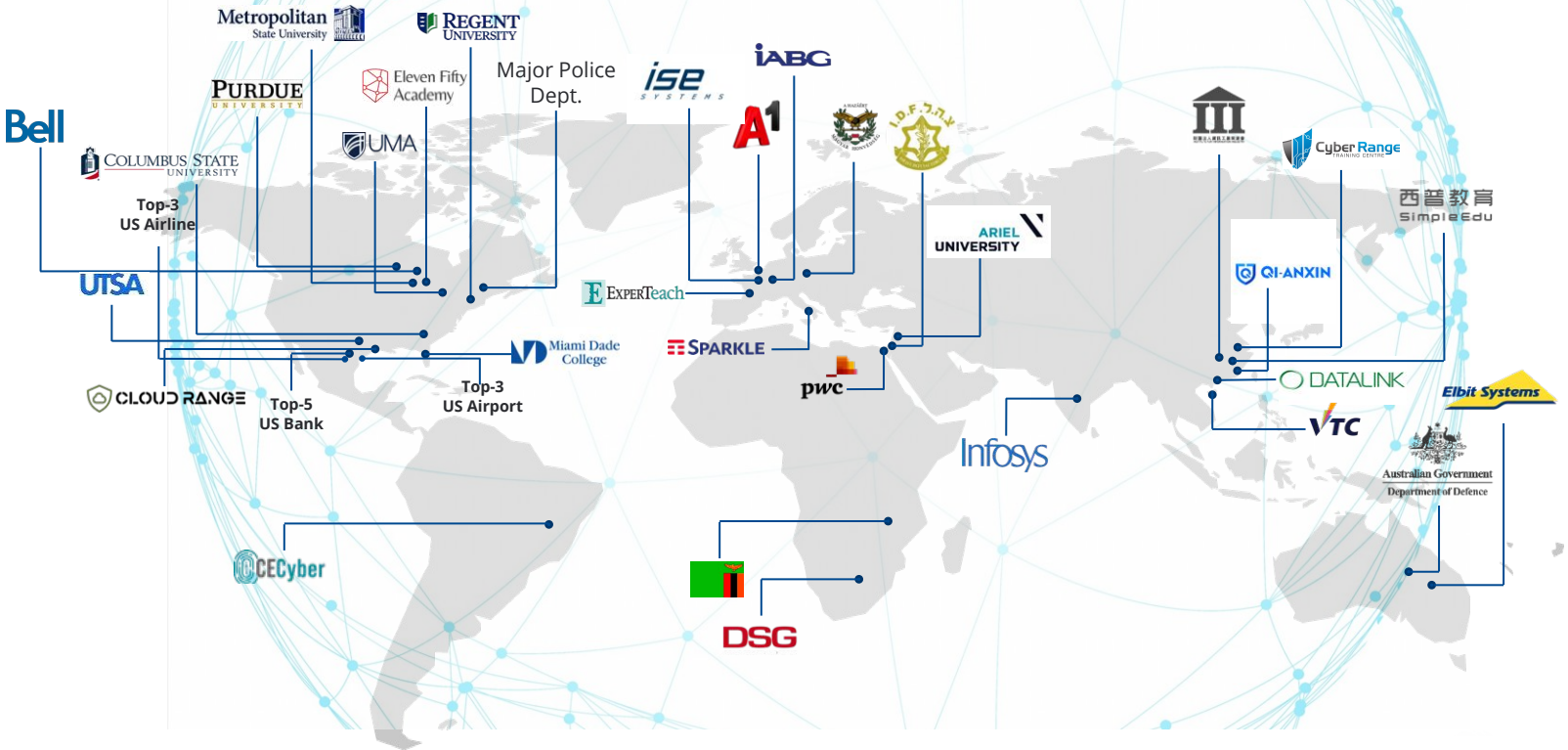
of cybersecurity professionals feel that their organization has been impacted by a shortage of skilled analysts.

Source: ESG/ISSA: The Life and Times of Cybersecurity Professionals, April 2019

We believe in Experiential Learning

CYBERBIT
TRAIN FOR REAL

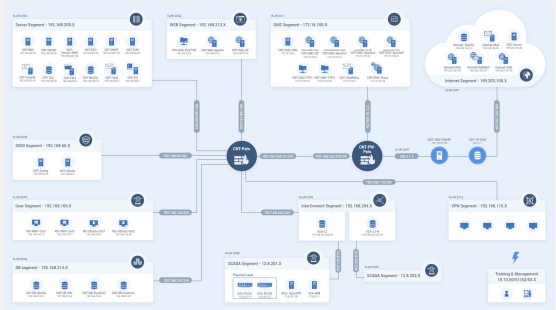
The Most Widely Used Cybersecurity Training Platform



Cyberbit Range: Hyper-Realistic Training

Simulating a Real-World SOC Under Attack

Real World Networks



Market-leading security tools

IBM

McAfee

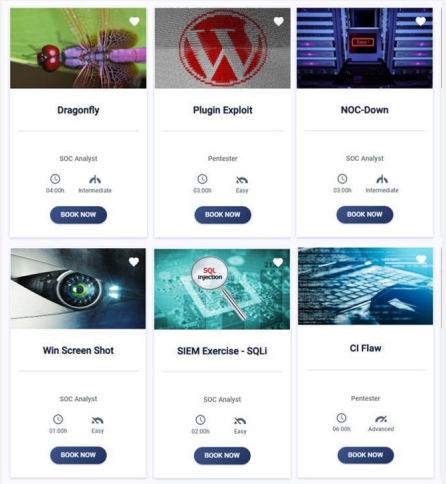
paloalto NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD

splunk>

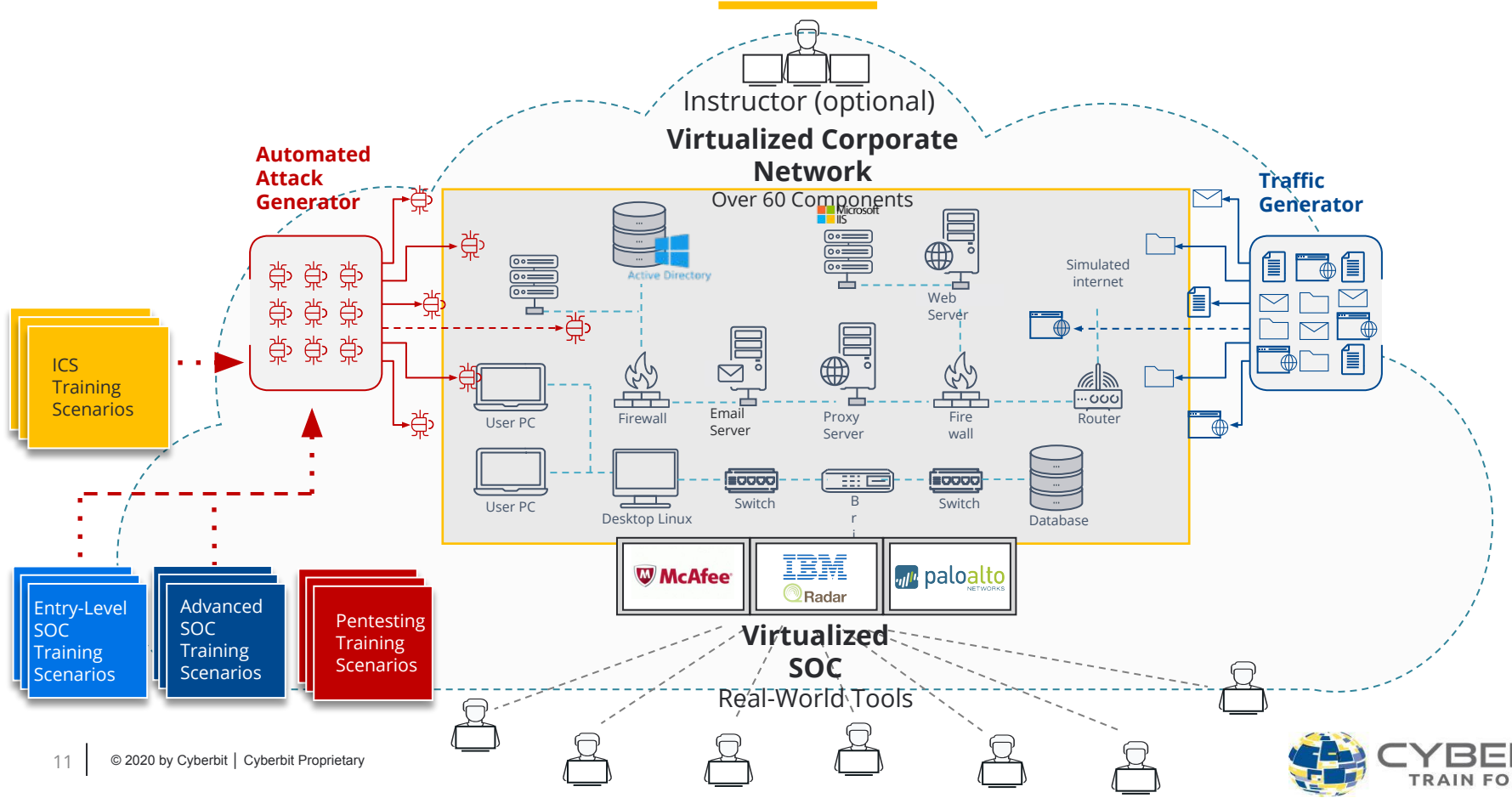
ArcSight

Real-World cyberattacks



CYBERBIT TRAIN FOR REAL

Cyber Range Hyper Realistic Environment



CYBERBIT
TRAIN FOR REAL

Training Exercises for Any Use

Dragonfly

SOC Analyst

04:00h | Intermediate

BOOK NOW

Plugin Exploit

Pentester

03:00h | Easy

BOOK NOW

NOC-Down

SOC Analyst

03:00h | Intermediate

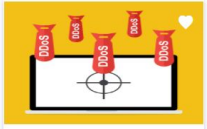
BOOK NOW

DDOS SYN Flood

SOC Analyst

01:00h | Easy

BOOK NOW



DDOS DNS Amplification

SOC Analyst

02:00h | Intermediate

BOOK NOW

Firewall Vulnerability Scanning

SOC Analyst

01:00h | Easy

BOOK NOW

Fileless Techniques

SOC Analyst

04:00h | Advanced

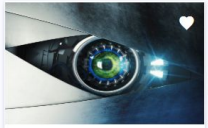
BOOK NOW

WMI Worm

SOC Analyst

04:00h | Advanced

BOOK NOW



Win Screen Shot

SOC Analyst

01:00h | Easy

BOOK NOW

SIEM Exercise - SQLi

SOC Analyst

02:00h | Easy

BOOK NOW

CI Flaw

Pentester

06:00h | Advanced

BOOK NOW

Domain Keylogger

SOC Analyst

02:00h | Intermediate

BOOK NOW

Customer Data Exfiltration

Pentester

03:00h | Intermediate

BOOK NOW

WPAD MiTM

SOC Analyst

03:00h | Advanced

BOOK NOW

VBLeaks

SOC Analyst

03:00h | Intermediate

BOOK NOW

Share-Lock Ransomware

SOC Analyst

04:00h | Advanced

BOOK NOW

Killer Trojan

Golden Ticket

Email Dumper

DB Dump FTP Exploit

Trojan Share Privilege Escalation

Apache Shutdown

Encrypted Data Intercept

Apache Web Defacement

Diverse Use Cases

Federico Italiano
Pasquale Raia

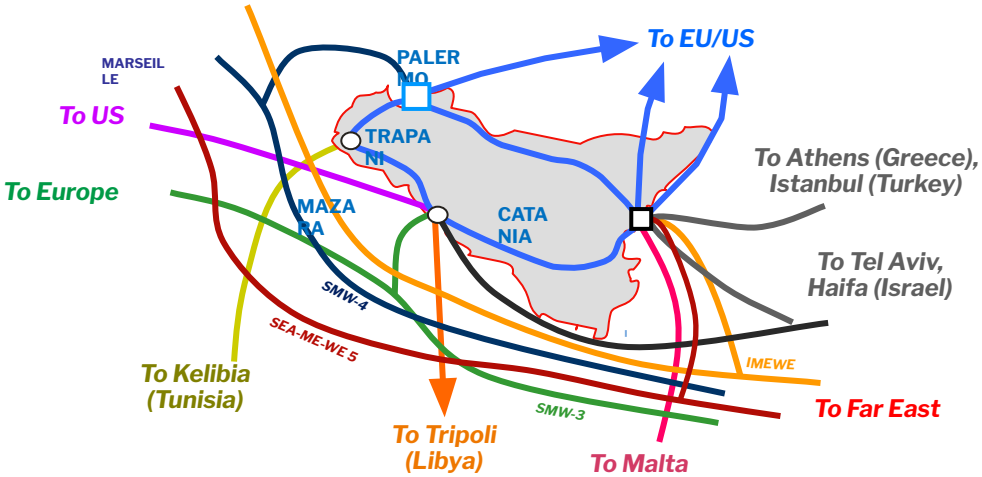
Sparkle Sicily Hub: il punto d'incontro della connettività di Sparkle in Italia

19 cavi sottomarini internazionali atterrano in

Sicilia verso:

PALERMO
CATANIA
MAZARA
TRAPANI
POZZALLO

Per la sua posizione centrale nel Mediterraneo, la Sicilia é il cuore italiano dell'infrastruttura di Sparkle con l'ecosistema detto Sicily Hub:
11 cavi internazionali (verso Americhe, Nord-Africa, Medio-Oriente e Far East)
5 Landing stations
2 Datacenters: Catania e Palermo



— BlueMed — Already existing cables

SPARKLE

La vision: Sparkle Sicily Hub come Polo di servizi di Security

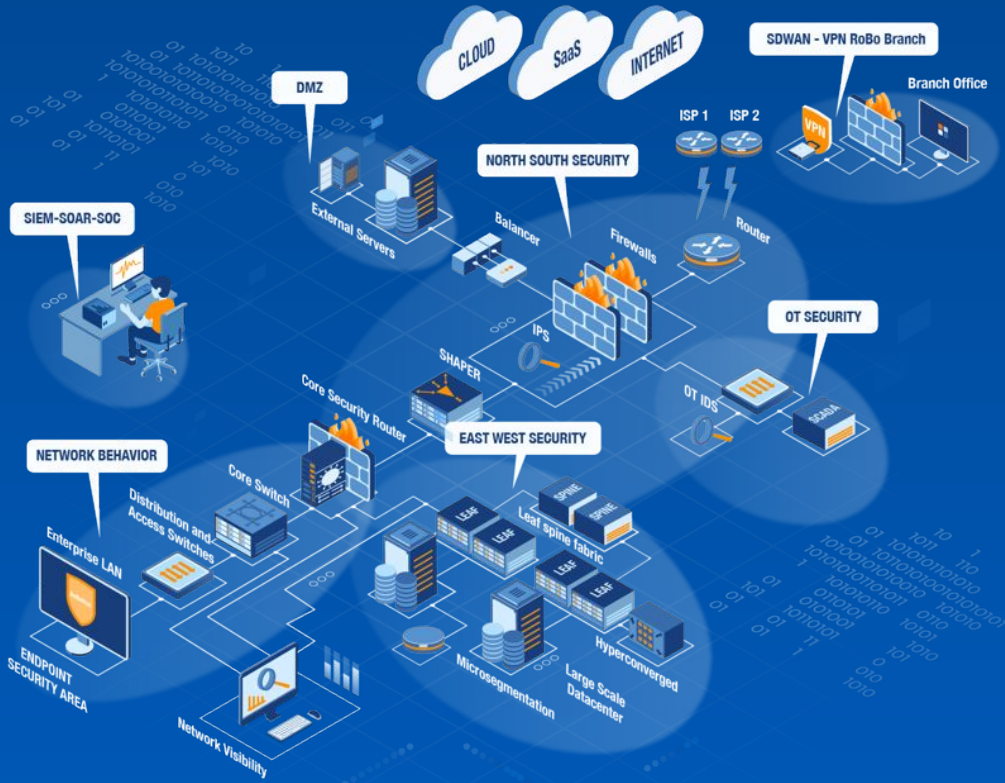
SICUREZZA INTERNA

SERVIZI DI SICUREZZA PER IL MERCATO SAAS

- Back-up — rubrik
- Disaster Recovery — NUTANIX, rubrik
- Cybersecurity Simulation Platform — CYBERBIT PROTECTING A NEW DIMENSION

Cyber Range

Detect, respond and recover from a Security Incident



Andrea Dainese (CSO @ NGS)

andrea.dainese@nextgensolutions.it

- Senior Network & Security Architect with 15+ years' experience in management of complex IT infrastructures
- Focused on cyber security strategies, GDPR/ISO27001 compliance and automation
- Member of Cyber Incident Response Team
- Cisco (CCIE), VMware, Red Hat… certified
- Privacy and digital security evangelist – expert counselor-mediator in Cyberbullying

Rosario Bonanno (SE @ Cyberbit)

rosario.bonanno@cyberbit.com

Rosario is a Cybersecurity professional with around 20 years of experience. Rosario is the South Europe Cyberbit **Sales Engineer** and **Cyber Range Instructor**. Prior to Cyberbit Sales Engineer Rosario was part of Symantec System Engineer Team Responsible for the end-to-end technical engagement with Symantec large customers and partners.

Objectives

- Understand how Cyber Range can help your SOC
- Learn how to approach a security incident
- Understand how to optimize incident analysis

- Learn from any security incident

Typical SOC Operation

People

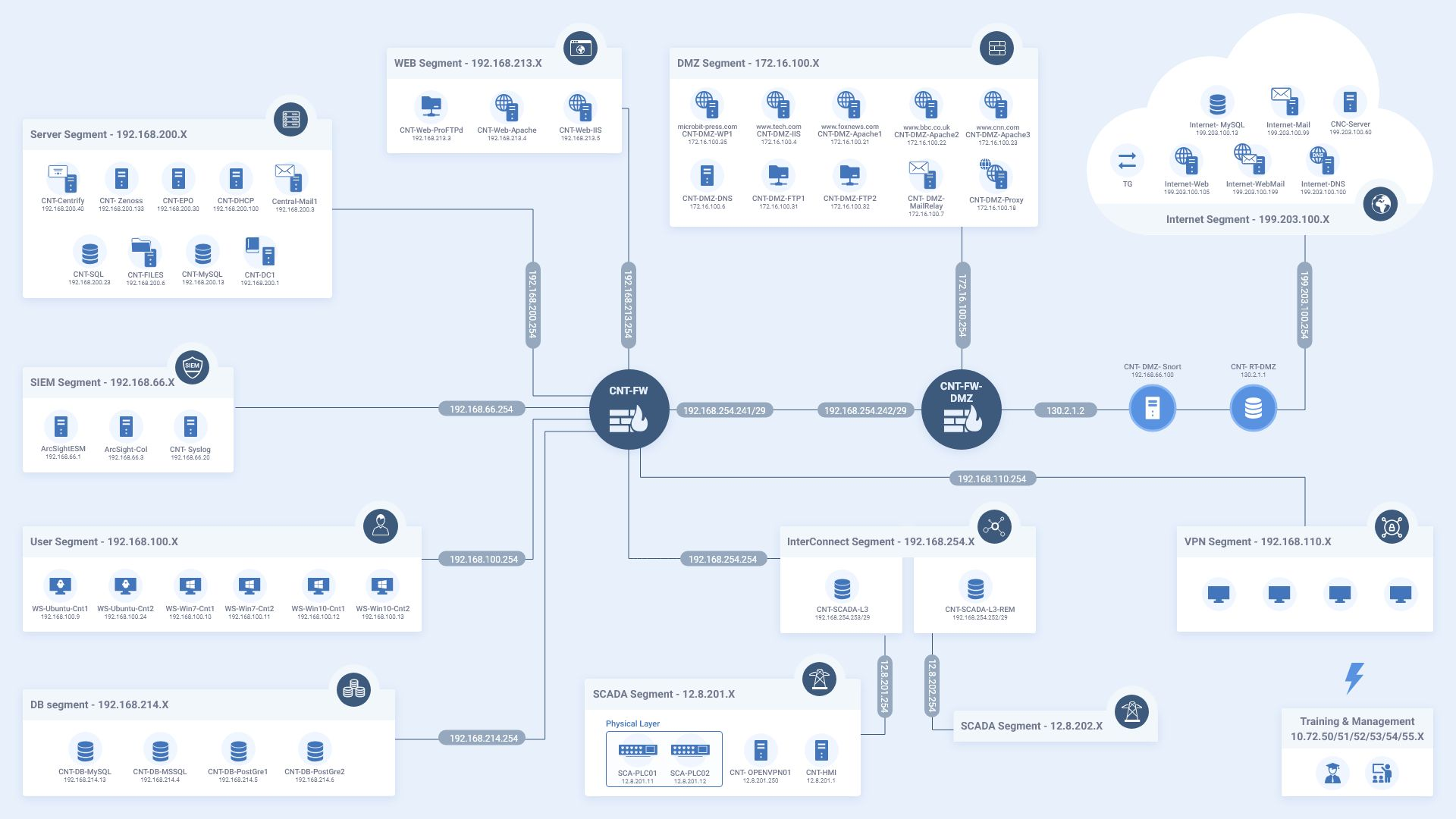
- Analyst (Tier 1)
  Triage Specialist
- Security Analyst (Tier 2)
  Incident responder
- Expert Analyst (Tier 3)
  Threat Hunter / Pentester
- SOC Manager (Tier 4)

Processes

- Event Classification
- Prioritization and analysis
- Remediation and recovery
- Assessment & Audit

Tools

- Asset Discovery
- SIEM
- Firewall
- Endpoint protection
- Threat intelligence
- Network Forensics
- Pentesting [...]


WEB Segment - 192.168.213.X
CNT-Web-ProFTPd
192.168.213.3
CNT-Web-Apache
192.168.213.4
CNT-Web-IIS
192.168.213.5
DMZ Segment - 172.16.100.X
microbit-press.com
CNT-DMZ-WP1
172.16.100.95
www.tech.com
CNT-DMZ-IIS
172.16.100.4
www.foxnews.com
CNT-DMZ-Apache1
172.16.100.21
www.bbc.co.uk
CNT-DMZ-Apache2
172.16.100.22
www.cnn.com
CNT-DMZ-Apache3
172.16.100.23
CNT-DMZ-DNS
172.16.100.6
CNT-DMZ-FTP1
172.16.100.81
CNT-DMZ-FTP2
172.16.100.82
CNT- DMZ-MailRelay
172.16.100.7
CNT-DMZ-Proxy
172.16.100.18
Internet- MySQL
199.203.100.13
Internet-Mail
199.203.100.99
CNC-Server
199.203.100.60
TG
Internet-Web
199.203.100.105
Internet-WebMail
199.203.100.199
Internet-DNS
199.203.100.100
Internet Segment - 199.203.100.X
Server Segment - 192.168.200.X
CNT-Centrify
192.168.200.40
CNT- Zenoss
192.168.200.133
CNT-EPO
192.168.200.30
CNT-DHCP
192.168.200.100
Central-Mail1
192.168.200.3
CNT-SQL
192.168.200.23
CNT-FILES
192.168.200.6
CNT-MySQL
192.168.200.13
CNT-DC1
192.168.200.1
192.168.200.254
192.168.213.254
172.16.100.254
199.203.100.254
SIEM Segment - 192.168.66.X
ArcSightESM
192.168.66.1
ArcSight-Col
192.168.66.3
CNT- Syslog
192.168.66.20
192.168.66.254
CNT-FW
192.168.254.241/29
192.168.254.242/29
CNT-FW-DMZ
130.2.1.2
CNT- DMZ- Snort
192.168.66.100
CNT- RT-DMZ
130.2.1.1
192.168.110.254
User Segment - 192.168.100.X
WS-Ubuntu-Cnt1
192.168.100.9
WS-Ubuntu-Cnt2
192.168.100.24
WS-Win7-Cnt1
192.168.100.10
WS-Win7-Cnt2
192.168.100.11
WS-Win10-Cnt1
192.168.100.12
WS-Win10-Cnt2
192.168.100.13
192.168.100.254
192.168.254.254
InterConnect Segment - 192.168.254.X
CNT-SCADA-L3
192.168.254.253/29
CNT-SCADA-L3-REM
192.168.254.252/29
VPN Segment - 192.168.110.X
DB segment - 192.168.214.X
CNT-DB-MySQL
192.168.214.13
CNT-DB-MSSQL
192.168.214.4
CNT-DB-PostGre1
192.168.214.5
CNT-DB-PostGre2
192.168.214.6
192.168.214.254
SCADA Segment - 12.8.201.X
Physical Layer
SCA-PLC01
12.8.201.11
SCA-PLC02
12.8.201.12
CNT- OPENVPN01
12.8.201.250
CNT-HMI
12.8.201.1
12.8.201.254
12.8.202.254
SCADA Segment - 12.8.202.X
Training & Management
10.72.50/51/52/53/54/55.X

0

Detection

Daily Analysis

- Daily activity of SOC operators starts from the SIEM:

	Id	Description	Offense Type	Offense Source	Magnitude

No results were returned.

- Regular check should verify the effectiveness of the in place rules:

Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP
71	Sep 11, 2020, 1:19:02 PM	Firewall Session Closed	172.16.100.35	47246	192.168.214.13
1	Sep 11, 2020, 1:19:02 PM	Firewall Session Closed	172.16.100.35	47182	192.168.214.13
1	Sep 11, 2020, 1:18:58 PM	Firewall Session Closed	172.16.100.35	47174	192.168.214.13
1	Sep 11, 2020, 1:18:57 PM	Firewall Session Closed	172.16.100.35	47174	192.168.214.13

- Anomaly connection from Wordpress server to MySQL server (with payment data)

Confirm the anomaly

- Anomaly detected: Wordpress website is connecting to the credit card database:

09/11 13:19:02	end	CNT-DMZ	CNT-DMZ	172.16.100.35		192.168.214.13	3306	mysql	allow
09/11 13:19:02	end	CNT-DMZ	CNT-DMZ	172.16.100.35		192.168.214.13	3306	mysql	allow
09/11 13:19:01	end	CNT-DMZ	CNT-DMZ	172.16.100.35		192.168.214.13	3306	mysql	allow
09/11 13:19:01	end	CNT-DMZ	CNT-DMZ	172.16.100.35		192.168.214.13	3306	mysql	allow
09/11 13:19:01	end	CNT-DMZ	CNT-DMZ	172.16.100.35		192.168.214.13	3306	mysql	allow
09/11 13:19:01	end	CNT-DMZ	CNT-DMZ	172.16.100.35		192.168.214.13	3306	mysql	allow

- What is going on? (attack, administrative activity, misconfiguration)

0

Analysis

What is going on in the database server?

- MySQL server analysis: /var/log/mysql/error.log

```
2020-09-11T13:18:47.310572Z 25 [Note] Access denied for user 'root'@'microbit-pr
ess' (using password: YES)
2020-09-11T13:18:47.314561Z 26 [Note] Access denied for user 'root'@'microbit-pr
ess' (using password: YES)
2020-09-11T13:18:47.318313Z 27 [Note] Access denied for user 'root'@'microbit-pr
ess' (using password: YES)
2020-09-11T13:18:47.322056Z 28 [Note] Access denied for user 'root'@'microbit-pr
ess' (using password: YES)
2020-09-11T13:18:47.326067Z 29 [Note] Access denied for user 'root'@'microbit-pr
ess' (using password: YES)
2020-09-11T13:18:47.329825Z 30 [Note] Access denied for user 'root'@'microbit-pr
ess' (using password: YES)
```

- Brute force attack detected
- Does the attacker gained access to the database?

Data has been leaked?

- MySQL server analysis: /var/log/mysql/mysql.log

```
2020-09-11T13:18:47.351779Z         36 Connect   root@microbit-press on  using TC
P/IP
2020-09-11T13:18:47.356424Z         36 Query     SHOW DATABASES
2020-09-11T13:18:47.368160Z         36 Quit
2020-09-11T13:18:52.633412Z         37 Connect   root@microbit-press on  using TC
P/IP
2020-09-11T13:18:52.642958Z         37 Query     select @@version_comment limit 1
2020-09-11T13:18:52.645388Z         37 Query     show tables in bookshop
2020-09-11T13:18:52.646579Z         37 Quit
2020-09-11T13:18:52.675627Z         38 Connect   root@microbit-press on  using TC
P/IP
2020-09-11T13:18:52.676344Z         38 Query     select @@version_comment limit 1
2020-09-11T13:18:52.677077Z         38 Query     select * from bookshop.payments
```

- Access granted
- Data leaked (payment table with credit card information)

Timeline (1)

- 13:18:02 Wordpress server to MySQL connections detected (brute force)
- 13:18:47 MySQL access granted (root user from Wordpress server)
- 13:18:52 MySQL data leak (payments table)

Wordpress server has been compromised?

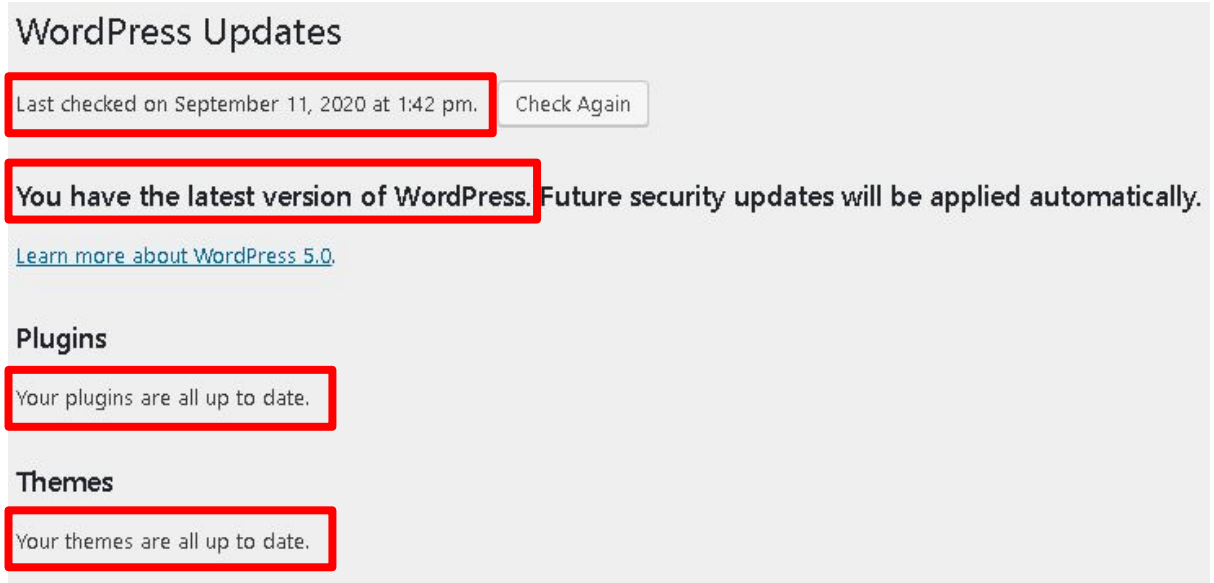
- Wordpress server analysis:

```
root@CNT-DMZ-WP1:~# find /var/www/html/ -mtime -1 -type f -ls
  1183571      4 -rw-r--r--   1 www-data www-data      114 Sep 11 13:18 /var/www
/html/wp-content/uploads/image.php
  1183572      4 -rw-r--r--   1 www-data www-data      637 Sep 11 13:18 /var/www
/html/wp-content/uploads/test.php
  1183573      4 -rw-r--r--   1 www-data www-data      387 Sep 11 13:18 /var/www
/html/wp-content/uploads/passwords.txt
```

- Recent files found:
  - image.php: web shell
  - test.php: brute force attack script
  - passwords.txt: password dictionary
- Files are malicious

How have been the files uploaded? (1)

- Wordpress application analysis:



- No updates available: has been used a zero day vulnerability?

How have been the files uploaded? (2)

- Wordpress application analysis:

- Vulnerability assessment: https://www.exploit-db.com/

- Vulnerable application (arbitrary file upload)

How the malicious files have been used?

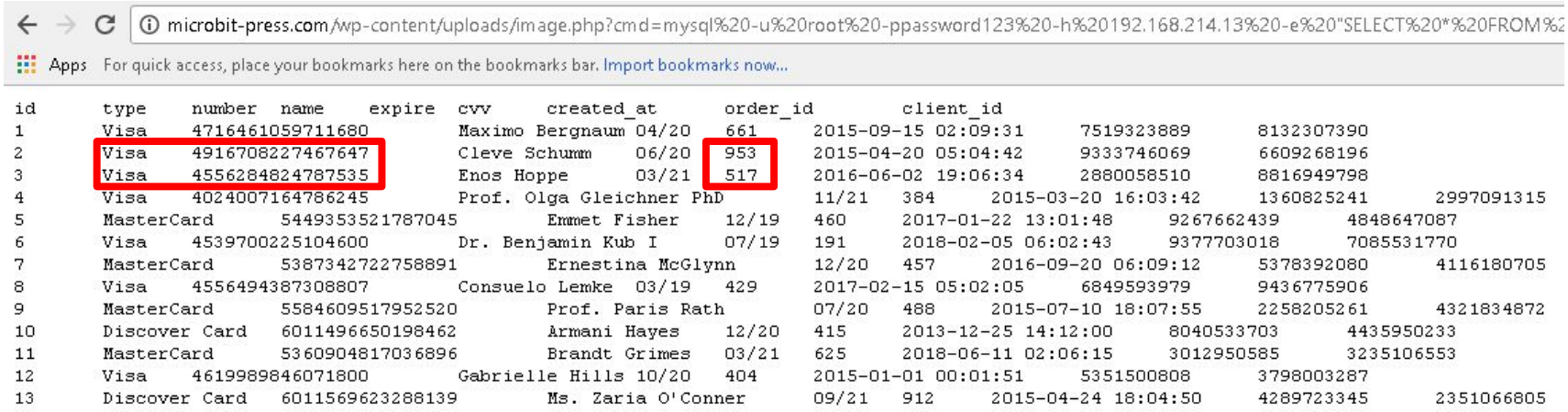
- Webserver log analysis: /var/log/nginx/access.log

```
199.203.100.66 - - [11/Sep/2020:13:18:31 +0000] "GET /wp-content/uploads/image.p
hp?cmd=netstat%20-tun HTTP/1.1" 200 305 "-" "Mozilla/5.0 (X11; Linux x86_64) App
leWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"
199.203.100.66 - - [11/Sep/2020:13:18:31 +0000] "GET /wp-content/uploads/image.p
hp?cmd=ping%20-c%201%20192.168.214.13 HTTP/1.1" 200 294 "-" "Mozilla/5.0 (X11; L
inux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/
537.36"
199.203.100.66 - - [11/Sep/2020:13:18:41 +0000] "GET /wp-content/uploads/image.p
hp?cmd=nc%20192.168.214.13%203306%20%3C%20%2Fdev%2Fnull HTTP/1.1" 200 121 "-" "M
ozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.
0.2704.103 Safari/537.36"
```

- Command executed: ls, arp, netstat, ping, nc, mysql
- Data leak confirmed

Data leak confirmation

- Executing mysql command using the malicious web shell: /wp-content/uploads/image.php?cmd=mysql -u root -ppassword123 -h 192.168.214.13 -e "select * from bookshop.payments"



id	type	number	name	expire	cvv	created_at	order_id	client_id			
1	Visa	4716461059711680	Maximo Bergnaum	04/20	661	2015-09-15 02:09:31	7519323889	8132307390			
2	Visa	4916708227467647	Cleve Schumm	06/20	953	2015-04-20 05:04:42	9333746069	6609268196			
3	Visa	4556284824787535	Enos Hoppe	03/21	517	2016-06-02 19:06:34	2880058510	8816949798			
4	Visa	4024007164786245	Prof. Olga Gleichner PhD		11/21	384	2015-03-20 16:03:42	1360825241	2997091315		
5	MasterCard	5449353521787045	Emmet Fisher	12/19	460	2017-01-22 13:01:48	9267662439	4848647087			
6	Visa	4539700225104600	Dr. Benjamin Kub I	07/19	191	2018-02-05 06:02:43	9377703018	7085531770			
7	MasterCard	5387342722758891	Ernestina McGlynn		12/20	457	2016-09-20 06:09:12	5378392080	4116180705		
8	Visa	4556494387308807	Consuelo Lemke	03/19	429	2017-02-15 05:02:05	6849593979	9436775906			
9	MasterCard	5584609517952520	Prof. Paris Rath		07/20	488	2015-07-10 18:07:55	2258205261	4321834872		
10	Discover Card	6011496650198462	Armani Hayes	12/20	415	2013-12-25 14:12:00	8040533703	4435950233			
11	MasterCard	5360904817036896	Brandt Grimes	03/21	625	2018-06-11 02:06:15	3012950585	3235106553			
12	Visa	4619989846071800	Gabrielle Hills	10/20	404	2015-01-01 00:01:51	5351500808	3798003287			
13	Discover Card	6011569623288139	Ms. Zaria O'Conner		09/21	912	2015-04-24 18:04:50	4289723345	2351066805		

- Data leak confirmed

When the malicious files have been uploaded?

- Webserver log analysis: /var/log/nginx/access.log

```
199.203.100.66 - - [11/Sep/2020:13:18:21 +0000] "POST /wp-content/plugins/reflex
-gallery/admin/scripts/FileUploader/php.php HTTP/1.1" 200 56 "-" "curl/7.58.0"
199.203.100.66 - - [11/Sep/2020:13:18:47 +0000] "POST /wp-content/plugins/reflex
-gallery/admin/scripts/FileUploader/php.php HTTP/1.1" 200 55 "-" "curl/7.58.0"
199.203.100.66 - - [11/Sep/2020:13:18:47 +0000] "POST /wp-content/plugins/reflex
-gallery/admin/scripts/FileUploader/php.php HTTP/1.1" 200 60 "-" "curl/7.58.0"
```

- Attacker IP found (Israel)

Could other servers have been compromised too?

- Firewall log analysis:

199.203.100.66	51836	172.16.100.35	80
199.203.100.66	51840	130.2.1.35	80
199.203.100.66	51844	172.16.100.35	80
199.203.100.66	51840	172.16.100.35	80
199.203.100.66	51846	172.16.100.35	80
199.203.100.66	51842	130.2.1.35	80
199.203.100.66	51838	172.16.100.35	80

- Attack targeted Wordpress server only

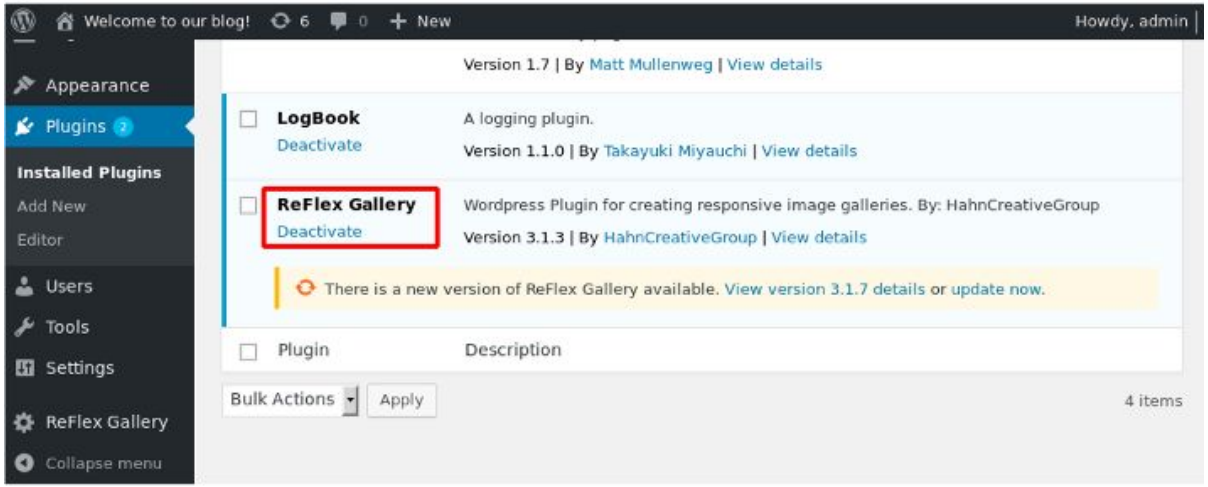
Timeline (2)

- 13:18:21 Malicious files upload (Reflex Gallery Wordpress plugin exploit)
- 13:18:47 Wordpress server to MySQL connections detected (brute force)
- 13:18:47 MySQL access granted (root user from Wordpress server)
- 13:18:52 MySQL data leak (payments table)

Remediation

Wordpress application

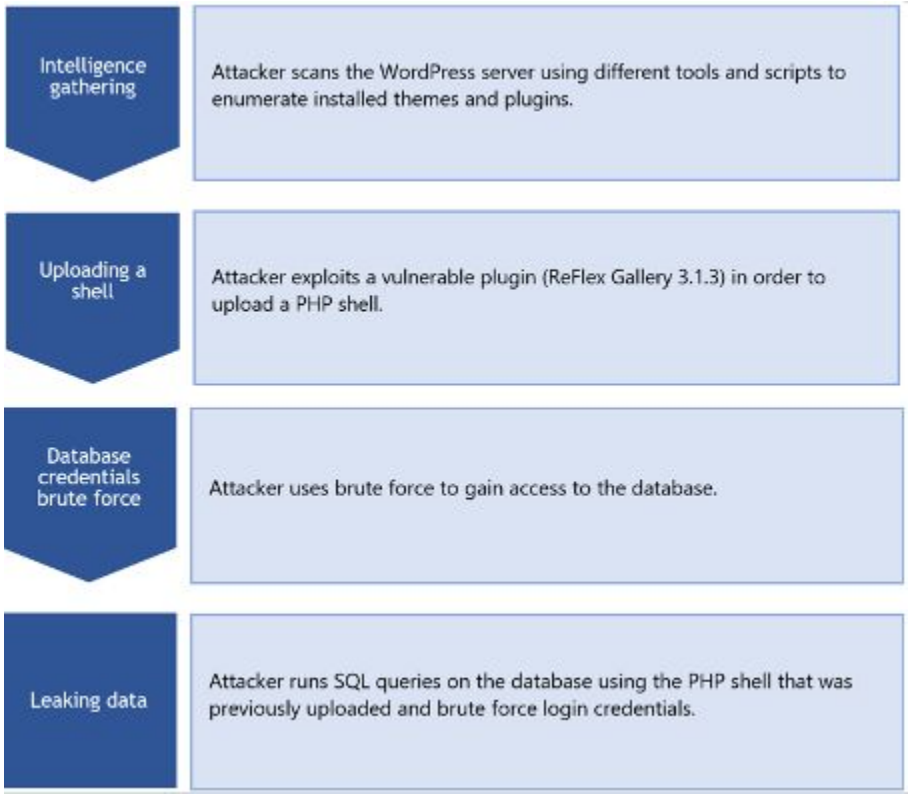
- Delete or update Wordpress plugins: Wordpress is not considered a weak application; the misuse of plugins and themes make it vulnerable.
- Delete the webshell (Wordpress server)
- Change MySQL root password (MySQL server): a weak password leads to account compromise



Lesson Learned
(Post Mortem Analysis)

Attack Flow

1. A Wordpress website is exposed to Internet.
2. A vulnerable Wordpress plugin has been used to upload a webshell.
3. The webshell has been used to find the database administrative password.
4. The administrative account has been used to leak sensitive information.



Attack Kill Chain (how to stop the attack) (1)

1. A vulnerable application can be used to compromise critical servers:
   a. Reduce attack surface
   b. Patch management (kill #2)
   c. Vulnerability Assessment and Penetration test (kill #2)
   d. Hardening (disable PHP Exec) (kill #3)
   e. CMS generators (Wordpress WP2Static plugin) (kill #1,2)
2. Weak passwords can be easily discovered
   a. Use complex passwords (kill #3)
   b. Use password management softwares (not XLS/TXT files) (kill #3)
3. Zero trust networks:
   a. Enable required traffic flows only (kill #3)
   b. Review firewall policies (kill #3)
   c. Enable per database access from specific hosts (MySQL permissions) (kill #3,4)
   d. Split critical data into different servers (already implemented) (kill #3,4)

Attack Kill Chain (how to stop the attack) (2)

4. Install a Web Application Firewall
   a. Filter out anomaly web requests (kill #2)
5. Improve incident detection:
   a. Enable Firewall IPS (kill #3)
   b. Assess and review SIEM rules
   c. Implement a PDCA framework (kill #1,2,3,4)
6. Compliance:
   a. PCI DSS (CVV cannot be stored)

NGS

SECURITY FREEDOM

www.nextgensolutions.it

NGS S.r.l. - 15° piano Torre Net, interni C-D - Piazza Aldo Moro 10, 35129 Padova - tel. +39 0498257376 / fax +39 0498252590