



TALLINNA TEHNIKAÜLIKOOL
INSENERITEADUSKOND
Virumaa kolledž

Digitaalse kohtuekspertiisi kasutamine sissetungijate jälgede otsimiseks

Using digital forensics to search for traces of intruders

ARUKAD SÜSTEEMID JA RAKENDUSINFOTEHNOLOOGIA ÕPPEKAVA
LÕPUTÖÖ

Üliõpilane: Valentin Mihhaiski

Üliõpilaskood: 183579

Juhendaja: Larissa Joonas, Lektor

AUTORIDEKLARATSIOON

Olen koostanud lõputöö iseseisvalt.

Lõputöö alusel ei ole varem kutse- või teaduskraadi või inseneridiplomit taotletud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

LIHTLITSENTS LÕPUTÖÖ ÜLDSUSELE KÄTTESAADAVAKS TEGEMISEKS JA REPRODUTSEERIMISEKS

Mina Valentin Mihhaiski (sünnikuupäev: 28.02.1999)

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Digitaalse kohtuekspertiisi kasutamine sissetungijate jälgede otsimiseks“, mille juhendaja on Larissa Joonas,

1.1. reprodutseerimiseks säilitamise ja elektroonilise avaldamise eesmärgil, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. Olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta kolmandate isikute intellektuaalomandi ega isikuandmete kaitse seadusest ja teistest õigusaktidest tulenevaid õigus

SISUKORD

EESSÖNA.....	7
LÜHENDITE JA TÄHISTE LOETELU.....	8
SISSEJUHATUS.....	9
1. HAAVATAVUSE ANALÜÜS.....	10
1.1. IT turvalisus analüüs	10
1.2. Häkkerid	11
1.3. Mälu	12
2. STSENAARIUM	13
2.1. MITRE ATT&CK®	13
2.2. Häkkeri profiil	29
2.3. Häkkerite tegevus stsenaarium	29
2.4. Stsenaarium operatsioonisüsteemi pahatahtliku mõju jälgede leidmiseks	30
3. MÄLUPILTI LOOMINE JA ANALÜÜSEERIMINE.....	31
3.1. MÄLUPILT	31
3.2. RAM-pildi loomise rakenduste analüüs ja võrdlus	31
3.3. Mälupilt loomine	31
3.4. Mälupilti analüüseerimine	36
4. TÖÖTULEMUSED.....	39
KOKKUVÕTE.....	40
Summary.....	41
KASUTATUD KIRJANDUSE LOETELU	42

EESSÕNA

Digitaalse kohtuekspertiisi nagu tõeline kangelane teadusvaldkondade seas, paraneb ja areneb pidevalt. Kavalate kurjategijate ees püsimiseks on vaja pidevalt uuendada koolitusmeetodeid ja kasutada täiustatud seadmeid. Seega säilitab diskreetne kriminalistika oma asjakohasuse ja tähtsuse, kuid nõuab pidevat ajakohastamist ja kohanemist muutuvate tingimustega.

Tahan avaldada sügavat tänu õpetaja Larissa Joonasele abi eest tema algatusel koostatud lõputöö jaoks huvitava teema pakkumisel. Ja ka tänu tagasiside, nõuannete ja eest töö kirjutamise protsessis.

See teema tundus mulle huvitav, sest häkkimine ja küberrünnakud on kogu infotehnoloogiamailma kuum teema.

Samuti soovin tänada õpetaja Ingrid Prees.

LÜHENDITE JA TÄHISTE LOETELU

RAM	Meelevaldse juurdepääsuga mälu
ROM	Püsiv mälu
IT	Infotehnoloogia
FTK	Forensic Toolkit
ATT&CK	The Adversarial Tactics, Techniques, and Common Knowledge
USB	Universal Serial Bus

SISSEJUHATUS

Mälu kohtuekspertiis on analüüsimeetod, mis on levinud erinevates valdkondades, alates häkkimisjuhtumitele reageerimisest kuni pahavaraanalüüsini. See meetod võimaldab leida pahavara jälgi, kuid mõnel juhul aitab see ka mõista, kuidas sissetungija täpselt süsteemi ründab. Lõputöös lahendatakse probleem, kus sissetungijad, kes suutsid operatsioonisüsteemi häkkida ja seda märkamatult mõjutada, jäävad karistamata. Eesmärk on analüüsida arvuti RAM-i, mis on kokku puutunud pahavaraga, uurimaks operatsioonisüsteemi rünnakut ja leidmaks jälgi sissetungijate tegevusest. Valisin selle teema oma lõputöö jaoks, sest arvan, et see on hetkel äärmiselt asjakohane, arvestades, et maailmas on palju inimesi, kes ründavad süsteeme mitte ainult kasumi, vaid ka muude eesmärkide nimel. Elame maailmas, kus miski pole kindel peale muutuse, ja küberkuritegevus pole erand. Pidevalt arendatakse välja uusi ründemeetodeid, kirjutatakse ja testitakse sadu pahavara ning skriptid möödunud skanneritest, kontrollides veebist haavatavaid hoste ja avalikke teenuseid. Seetõttu on äärmiselt oluline püsida trendidega kursis ja omada oma arsenalis kõiki võimalikke tööriistu ja meetodeid, et olla sissetungijatega ühel lainepikkusel. [1]

Failirünneteta meetodeid kasutavate ohus osalejate arv on viimastel aastatel kasvanud. Sissetungijad ei hooli enam oma jalajälgede eemaldamisest, vaid püüavad need avastamise vältimiseks hoida võimalikult väikesed. See raskendab oluliselt infoturbspetsialistide tööd. Sisseehitatud tööriistade kasutamise ja skannitavate ROM-i pahatahtlike failide puudumise tõttu tähendab see, et mõned traditsioonilised turvalahendused ei pruugi olla kasulikud. [1]

Uurimisobjektiks on operatsioonisüsteemi WINDOWS 10 RAM-i mälu pilt.

Uuringu peamised eesmärgid:

Lua ainulaadne sissetungija tegevuse stsenaarium, mis on spetsiifiline konkreetsele olukorrale.

Tõhusama prügianalüüsi jaoks uurida sissetungijate tegevuste ja tehnikate standardeid MITRE ATT&CK®.

Leida parimad viisid mälu pilti loomiseks ja analüüsida neid.

Märksõnad: digikuritegevus, sissetungija, mälu pilt, häkkimine, bakalaureuse töö.

1. HAAVATAVUSE ANALÜÜS

1.1. IT TURVALISUSE ANALÜÜS

Esimese peatüki see osa kirjeldab, mis on IT-turvalisus ja miks seda vaja on.

IT-turvalisus kirjeldab ettevaatusabinõusid arvutite ja võrkude kaitsmiseks volitamata juurdepääsu eest. Need protsessid on loodud kaitsma häkkerite eest, kes võivad üritada süsteemiandmeid varastada või muul viisil murda.

IT-turvaohht on pahatahtlik tegu, mis kahjustab või varastab andmeid või häirib süsteeme.

See oht on tavaliselt nuhkvara, viirused, lunavara.

IT-haavatavus on IT-süsteemi haavatavus, mida sissetungija saab kasutada eduka rünnaku käivitamiseks. Need võivad tuleneda vigadest, funktsioonidest või kasutajaveast ning ründajad püüavad oma lõppeesmärgi saavutamiseks kasutada mõnda neist, sageli kombineerides ühte või mitut.[2]

IT-rünnakud on tegevused, mille eesmärk on infosüsteemi ressursside või teabe kogumine, hävitamine, ümbersuunamine, alandamine või hävitamine.



Joonis 1. IT-turvalisus

Joonisel 1. on näidatud et kui süsteemis on oht ja haavatavus, siis võib tekkida oht süsteemi kahjustada [3]

1.2. HÄKKERID

Küberturvalisuse statistika kohaselt toimub iga päev üle 2,200 küberrünnaku. Ja peaaegu igaühe taga on häkker, kes kasutab tehnilisi oskusi ja sotsiaalse inseneri taktikat, et kasutada ära turvaauke ja Interneti-kasutajaid nende kasuks.[3]

Häkker on nagu digitaalne detektiiv, kes kasutab oma oskusi arvutisüsteemide, võrkude ja tarkvara uurimiseks ning turvavigade avastamiseks, ära kasutamiseks või manipuleerimiseks.

Häkkerid jagunevad kolme põhikategooriasse: musta mütsi häkkerid, valge mütsi häkkerid ja halli mütsi häkkerid. Kuigi häkkerid kasutavad sageli turvaauke arvutitele, süsteemidele või võrkudele volitamata juurdepääsu saamiseks, ei ole kõik häkkimised pahatahtlikud ega ebaseaduslikud. [4]

Musta mütsi häkkerid on küberkurjategijad, kes tungivad pahatahtlikult süsteemidesse ebaseaduslikult. Musta häkkimise definitsioon on soov saada volitamata juurdepääs arvutisüsteemidele. Kui musta mütsi häkker leiab turvaauku, püüab ta seda ära kasutada, süstides sageli viirust või muud pahavara, näiteks trooja.[4]

Valge mütsi häkkerid on eetilised häkkerid, kes tuvastavad ja parandavad turvaauke. Häkkides süsteemidesse häkkivate organisatsioonide loal, püüavad valgekübarad häkkerid tuvastada süsteemi nõrkusi, et need parandada ja aidata tugevdada süsteemi üldist turvalisust.[4]

Halli mütsi häkkeritel ei pruugi olla musta mütsi häkkerite kuritegelikke või pahatahtlikke kavatsusi, kuid neil pole ka nende eelteadmisi ega nõusolekut, kelle süsteemi nad häkkivad. Kui aga hallikübara häkkerid avastavad nõrkusi, nagu nullpäeva haavatavused, annavad nad neist pigem teada kui kasutavad neid täielikult ära. Kuid halli mütsi häkkerid võivad nõuda tasu, et saada täielikku teavet avastatu kohta.[4]

Pärast süsteemi mõjutamist jätavad häkkerid mällu jäljed.



Joonis 2. Häkkeri anatoomia

Joonisel 2. on näidatud, et millised on häkkerite omadused [4]

1.3. MÄLU

Arvutimälu on arvutisüsteemi oluline osa, kus hoitakse andmeid ja käivitusprogramme. See võimaldab arvutil töötada, salvestades andmeid, mida hetkel kasutatakse või mis tulevikus vajalikud võivad olla.

Mälu on kahte tüüpi:

RAM – see muutmäluseade on muutlik mälu.

ROM - see on püsisalvestusvorm, on püsिमälu.

Kui soovid operatsioonisüsteemis sissetungija jälgi leida, siis on vaja luua mälupilt ja analüüsida RAM-mälu. See samm aitab avastada, mis täpselt süsteemis toimus vahetult enne kuriteo toimepanemist. Kuna kõik süsteemis toimivad protsessid salvestuvad RAM-i, on oluline see kätte saada enne arvuti väljalülitamist.

2. STSENAARIUM

Digitaalse häkkerdamise uurimisel mängib olulist rolli rünnaku stsenaariumi koostamine, mis määratleb sammude järjekorra, mida kasutatakse süsteemi kompromiteerimise analüüsimisel ja mõistmisel. See stsenaarium kirjeldab potentsiaalseid samme, mida võisid ründajad kasutada rünnaku toimepanemiseks, sealhulgas häkkimismeetodeid, kasutatud haavatavusi, tööriistu ja tehnikaid. Rünnaku stsenaariumi analüüs aitab uurijatel mõista, millised haavatavused on ära kasutatud, ning milliseid jälgi saab kasutada päritolu ja rünnaku olemuse väljaselgitamiseks. See võimaldab paremini kaitsta süsteemi tulevaste intsidentide eest ning välja töötada strateegiad sarnaste rünnakute ärahoidmiseks.

2.1. MITRE ATT&CK®

MITRE ATT&CK® on avalik teadmistebaas, mis põhineb tegelikel vaatlustel ja käsitleb sissetungija taktikaid ja meetodeid. ATT&CK teadmistebaasi kasutatakse erasektoris, valitsuses ja küberturbetoodete ning -teenuste kogukonnas konkreetsete ohumudelite ja meetodikate väljatöötamisel.[5]

MITRE ATT&CK® esmakordselt esitleti 2013. aastal. See loodi MITRE Corporationi poolt vastusena vajadusele parema ja põhjalikuma arusaamise järele taktikatest ja meetoditest, mida küberrünnakutes kasutatakse. Sestsaadik on see muutunud oluliseks töövahendiks küberkaitse valdkonnas, pakkudes väärtuslikke teadmisi ähvarduste analüüsiks ja infotehnoloogiasüsteemide kaitseseadete täiustamiseks.[5]

Reconnaissance

10 techniques

	Active Scanning (3)
	Gather Victim Host Information (4)
	Gather Victim Identity Information (3)
	Gather Victim Network Information (6)
	Gather Victim Org Information (4)
	Phishing for Information (4)
	Search Closed Sources (2)
	Search Open Technical Databases (5)
	Search Open Websites/Domains (3)
	Search Victim-Owned Websites

Joonis 3. Ettevõtte maatriks - Tutvumine

Tutvumise hõlmab meetodeid, mille käigus vastased koguvad aktiivselt või passiivselt teavet, mida saab kasutada sihtmärgi toetamiseks. See teave võib hõlmata üksikasju ohvriorganisatsiooni, infrastruktuuri või personali kohta. Vastane saab seda teavet kasutada, et toetada oma tegevust teistes elutsükli faasides, näiteks kasutada kogutud teavet esialgse juurdepääsu kavandamiseks ja teostamiseks, määrata kompromiteeritud eesmärkide ulatus ja tähtsus ning juhtida ja juhtida järgnevaid luuretegevusi.[6]

Resource Development 8 techniques

Acquire Access	
II	Acquire Infrastructure (8)
II	Compromise Accounts (3)
II	Compromise Infrastructure (7)
II	Develop Capabilities (4)
II	Establish Accounts (3)
II	Obtain Capabilities (6)
II	Stage Capabilities (6)

Joonis 4. Ettevõtte maatriks - Ressursside arendamine

Ressursiarendus koosneb tehnikatest, mis hõlmavad vastaseid, kes loovad, ostavad või kompromiteerivad/varastavad ressursse, mida saab kasutada sihtimise toetamiseks. Sellised ressursid hõlmavad infrastruktuuri, kontosid või võimalusi. Vastane saab neid ressursse kasutada abistamiseks vastase elutsükli teistes etappides, näiteks ostetud domeenide kasutamine käsu ja juhtimise toetamiseks, e-posti kontode andmepüügiks esialgse juurdepääsu osana või koodi allkirjastamise sertifikaatide varastamine kaitsest kõrvalehoidumise abistamiseks.[7]

Initial Access

10 techniques

Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)

Joonis 5. Ettevõtte maatriks - Esialgne juurdepääs

Esialgne juurdepääs koosneb tehnikatest, mis kasutavad erinevaid sisestusvektoreid, et saada oma esialgne tugi võrgus. Kohale jõudmiseks kasutatavad võtted hõlmavad sihipärast andmepüügi ja avalike veebiserverite nõrkade külgede ärakasutamist. Esialgse juurdepääsuga saavutatud tugipunktid võivad võimaldada jätkuvat juurdepääsu, nagu kehtivad kontod ja välise kaugteenuste kasutamine, või selle kasutamine võib olla piiratud paroolide muutmise tõttu.[8]

Execution

14 techniques

Cloud Administration Command
II Command and Scripting Interpreter (9)
Container Administration Command
Deploy Container
Exploitation for Client Execution
II Inter-Process Communication (3)
Native API
II Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Software Deployment Tools
II System Services (2)
II User Execution (3)
Windows Management Instrumentation

Joonis 6. Ettevõtte maatriks – Täitmine

Täitmine koosneb tehnikatest, mille tulemuseks on vastase juhitud kood, mis töötab kohalikus või kaugsüsteemis. Pahatahtlikku koodi käitavad tehnikad on sageli seotud kõigi teiste taktikate tehnikatega, et saavutada laiemad eesmärgid, nagu võrgu uurimine või andmete varastamine. Näiteks võib vastane kasutada kaugjuurdepääsu tööriista, et käivitada PowerShell skript, mis teeb süsteemi kaugtuvastust.[9]

Persistence	
20 techniques	
Account Manipulation (6)	
BITS Jobs	
Boot or Logon Autostart Execution (14)	
Boot or Logon Initialization Scripts (5)	
Browser Extensions	
Compromise Client Software Binary	
Create Account (3)	
Create or Modify System Process (4)	
Event Triggered Execution (16)	
External Remote Services	Power Settings
Hijack Execution Flow (12)	Pre-OS Boot (5)
Implant Internal Image	Scheduled Task/Job (5)
Modify Authentication Process (8)	Server Software Component (5)
Office Application Startup (6)	Traffic Signaling (2)
	Valid Accounts (4)

Joonis 7. Ettevõtte maatriks – Püsivus

Püsivus koosneb tehnikatest, mida vastased kasutavad süsteemidele juurdepääsu hoidmiseks taaskäivitamise, muudetud mandaatide ja muude katkestuste kaudu, mis võivad nende juurdepääsu katkestada. Püsivuse tagamiseks kasutatavad tehnikad hõlmavad mis tahes juurdepääsu, toiminguid või konfiguratsioonimuudatusi, mis võimaldavad neil süsteemides oma jalgealust säilitada, näiteks seadusliku koodi asendamine või kaaperdamine või käivituskoodi lisamine.[10]

Privilege Escalation

14 techniques

Abuse Elevation Control Mechanism (5)	
Access Token Manipulation (5)	
Account Manipulation (6)	
Boot or Logon Autostart Execution (14)	
Boot or Logon Initialization Scripts (5)	
Create or Modify System Process (4)	
Domain Policy Modification (2)	
Escape to Host	
Event Triggered Execution (16)	
Exploitation for Privilege Escalation	
Hijack Execution Flow (12)	
Process Injection (12)	
Scheduled Task/Job (5)	
Valid Accounts (4)	

Joonis 8. Ettevõtte maatriks - Privileegide tõstmine

Privileegide tõstmine hõlmab meetodeid, mida vastased kasutavad süsteemis või võrgus kõrgemate õiguste saamiseks. Sageli saavad vastased siseneda ja uurida võrku, millel on eelisõigusega juurdepääs, kuid nad vajavad oma eesmärkide saavutamiseks kõrgendatud õigusi. Levinud lähenemisviisid hõlmavad süsteemi haavatavuste, väärkonfiguratsioonide ja haavatavuste ära kasutamist.[11]

Defense Evasion	
43 techniques	
	Modify Registry
Abuse Elevation Control Mechanism (5)	Modify System Image (2)
Access Token Manipulation (5)	Network Boundary Bridging (1)
BITS Jobs	Obfuscated Files or Information (12)
Build Image on Host	Plist File Modification
Debugger Evasion	Pre-OS Boot (5)
Deobfuscate/Decode Files or Information	Process Injection (12)
Deploy Container	Reflective Code Loading
Direct Volume Access	Rogue Domain Controller
Domain Policy Modification (2)	Rootkit
Execution Guardrails (1)	Subvert Trust Controls (6)
Exploitation for Defense Evasion	System Binary Proxy Execution (13)
File and Directory Permissions Modification (2)	System Script Proxy Execution (1)
Hide Artifacts (11)	Template Injection
Hijack Execution Flow (12)	Traffic Signaling (2)
Impair Defenses (11)	Trusted Developer Utilities Proxy Execution (1)
Impersonation	Unused/Unsupported Cloud Regions
Indicator Removal (9)	Use Alternate Authentication Material (4)
Indirect Command Execution	Valid Accounts (4)
Masquerading (9)	Virtualization/Sandbox Evasion (3)
Modify Authentication Process (8)	Weaken Encryption (2)
Modify Cloud Compute Infrastructure (5)	XSL Script Processing

Joonis 9. Ettevõtte maatriks - Kaitsest kõrvalehoidmine

Kaitsest kõrvalehoidumine hõlmab tehnikaid, mida vastased kasutavad sissetungi ajal avastamise vältimiseks. Tuvastamise vältimiseks kasutatavate meetodite hulka kuuluvad viirusetõrjetarkvara kustutamine/keelamine või andmete ja skriptide

varjamine/krüptimine. Vastased kasutavad ja kuritarvitavad oma pahavara varjamiseks ka usaldusväärseid protsesse.[12]

Credential Access 17 techniques	
Adversary-in-the-Middle (3)	II
Brute Force (4)	II
Credentials from Password Stores (6)	II
Exploitation for Credential Access	
Forced Authentication	
Forge Web Credentials (2)	II
Input Capture (4)	II
Modify Authentication Process (8)	II
Multi-Factor Authentication Interception	
Multi-Factor Authentication Request Generation	
Network Sniffing	
OS Credential Dumping (8)	II
Steal Application Access Token	
Steal or Forge Authentication Certificates	
Steal or Forge Kerberos Tickets (4)	II
Steal Web Session Cookie	
Unsecured Credentials (8)	II

Joonis 10. Ettevõtte maatriks - Identimisteabe juurdepääs

Autentimise andmete hankimine hõlmab meetodeid, mille abil varastatakse autentimiseks vajalikke andmeid, nagu kasutajanimed ja paroolid. Autentimise

andmete hankimiseks kasutatavad tehnikad hõlmavad klahvivajutuste salvestamist või autentimisandmete mahavõtmist. Legitiimsete autentimise andmete kasutamine võib anda vastastele juurdepääsu süsteemidele, muutes nende tuvastamise raskemaks ja andes võimaluse luua rohkem kontosid, et aidata saavutada oma eesmärke.[13]

Discovery	
32 techniques	
Account Discovery (4)	II
Application Window Discovery	
Browser Information Discovery	
Cloud Infrastructure Discovery	
Cloud Service Dashboard	
Cloud Service Discovery	
Cloud Storage Object Discovery	
Container and Resource Discovery	
Debugger Evasion	
Device Driver Discovery	
Domain Trust Discovery	
File and Directory Discovery	
Group Policy Discovery	
Log Enumeration	
Network Service Discovery	
Network Share Discovery	
Network Sniffing	
Password Policy Discovery	
Peripheral Device Discovery	
Permission Groups Discovery (3)	II
Process Discovery	
Query Registry	
Remote System Discovery	
Software Discovery (1)	II
System Information Discovery	
System Location Discovery (1)	II
System Network Configuration Discovery (2)	II
System Network Connections Discovery	
System Owner/User Discovery	
System Service Discovery	
System Time Discovery	
Virtualization/Sandbox Evasion (3)	II

Joonis 11. Ettevõtte maatriks - Avastamine

Avastamine hõlmab tehnikaid, mida vastane võib kasutada süsteemi ja sisemise võrgu kohta teadmiste hankimiseks. Need tehnikad aitavad vastastel jälgida keskkonda ja orienteeruda enne otsustamist, kuidas tegutseda. Need võimaldavad vastastel uurida, mida nad saavad kontrollida, ja seda, mis asub nende sisenemispunkti ümber, et avastada, kuidas see võiks aidata neil praegust eesmärki saavutada. Tihti kasutatakse selleks eesmärgiks post-ründe teabe kogumiseks süsteemi enda operatsioonisüsteemi tööriistu.[14]

Lateral Movement

9 techniques

Exploitation of Remote Services	
Internal Spearphishing	
Lateral Tool Transfer	
Remote Service Session Hijacking (2)	
Remote Services (8)	
Replication Through Removable Media	
Software Deployment Tools	
Taint Shared Content	
Use Alternate Authentication Material (4)	

Joonis 12. Ettevõtte maatriks - Külgmise liikumine

Külgmised liigutused hõlmavad tehnikaid, mida vastased kasutavad võrgus kaugsüsteemidesse sisenemiseks ja neid kontrollimiseks. Enamikul juhtudel nõuab peamise eesmärgi täitmine võrgu uurimist, et leida oma sihtmärk ja seejärel sellele juurdepääsu saavutamist. Eesmärgi saavutamine hõlmab sageli mitme süsteemi ja konto kaudu pööramist. Vastased võivad paigaldada omaenda kaugjuhtimisvahendid, et läbi viia külgmised liigutused, või kasutada legitiimseid autentimisandmeid koos süsteemi enda võrgu- ja operatsioonisüsteemi tööriistadega, mis võivad olla varjatunud.[15]

Collection

17 techniques

Adversary-in-the-Middle (3)	II
Archive Collected Data (3)	II
Audio Capture	
Automated Collection	
Browser Session Hijacking	
Clipboard Data	
Data from Cloud Storage	
Data from Configuration Repository (2)	II
Data from Information Repositories (3)	II
Data from Local System	
Data from Network Shared Drive	
Data from Removable Media	
Data Staged (2)	II
Email Collection (3)	II
Input Capture (4)	II
Screen Capture	
Video Capture	

Joonis 13. Ettevõtte maatriks - Kogumine

Kogumine hõlmab tehnikaid, mida vastased võivad kasutada teabe kogumiseks ja teabeallikaid, kust teavet kogutakse, ning mis on seotud vastase eesmärkide täitmiseks. Sageli on järgmine eesmärk pärast andmete kogumist nende varastamine (eksfiltratsioon). Tavalised sihtallikad hõlmavad mitmesuguseid draivitüüpe, veebilehitsejaid, heli, videot ja e-kirju. Tavalised kogumismeetodid hõlmavad ekraanipiltide ja klaviatuurisendi salvestamist.[16]

Command and Control

17 techniques

Application Layer Protocol (4)	II
Communication Through Removable Media	
Content Injection	
Data Encoding (2)	II
Data Obfuscation (3)	II
Dynamic Resolution (3)	II
Encrypted Channel (2)	II
Fallback Channels	
Ingress Tool Transfer	
Multi-Stage Channels	
Non-Application Layer Protocol	
Non-Standard Port	
Protocol Tunneling	
Proxy (4)	II
Remote Access Software	
Traffic Signaling (2)	II
Web Service (3)	II

Joonis 14. Ettevõtte maatriks- Juhtimine ja kontroll

Juhtimine ja kontroll hõlmavad tehnikaid, mida vastased võivad kasutada suhtlemiseks süsteemidega, mida nad kontrollivad ohvri võrgus. Vastased püüavad tavaliselt jäljendada normaalset, oodatavat liiklust, et vältida avastamist. On

mitmeid viise, kuidas vastane saab luua juhtimise ja kontrolli erineva varjatuse tasemega, olenevalt ohvri võrgu struktuurist ja kaitsemeetmetest.[17]

Exfiltration

9 techniques

Automated Exfiltration (1)	II
Data Transfer Size Limits	
Exfiltration Over Alternative Protocol (3)	II
Exfiltration Over C2 Channel	
Exfiltration Over Other Network Medium (1)	II
Exfiltration Over Physical Medium (1)	II
Exfiltration Over Web Service (4)	II
Scheduled Transfer	
Transfer Data to Cloud Account	

Joonis 15. Ettevõtte maatriks- Väljafiltratsioon

Väljafiltratsioon hõlmab tehnikaid, mida vastased võivad kasutada andmete varastamiseks teie võrgust. Kui nad on andmed kogunud, pakendavad vastased need sageli nii, et vältida avastamist, samal ajal neid eemaldades. See võib hõlmata andmete kokkusurumist ja krüpteerimist. Andmete saamise tehnikad sihtmärgi võrgust hõlmavad tavaliselt nende ülekandmist nende käskude ja kontrolli kanali või alternatiivse kanali kaudu ning võivad hõlmata ka edastusele suuruse piiride seadmist.[18]

Impact

14 techniques

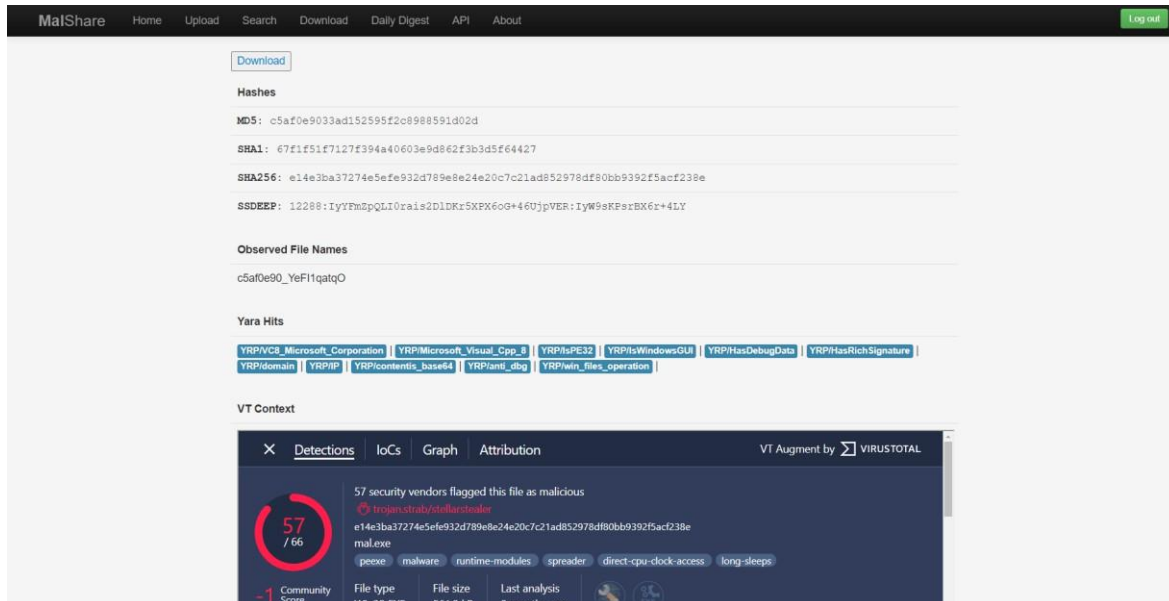
Account Access Removal	
Data Destruction	
Data Encrypted for Impact	
Data Manipulation (3)	
Defacement (2)	
Disk Wipe (2)	
Endpoint Denial of Service (4)	
Financial Theft	
Firmware Corruption	
Inhibit System Recovery	
Network Denial of Service (2)	
Resource Hijacking	
Service Stop	
System Shutdown/Reboot	

Joonis 16. Ettevõtte maatriks- Mõju

Mõju hõlmab erinevaid meetodeid, mida vastased rakendavad, et segada kättesaadavust või ohustada terviklikkust, manipuleerides äriliste ja operatiivprotsessidega. Selleks võidakse kasutada mitmesuguseid tehnikaid, näiteks andmete hävitamist või manipuleerimist. Mõnikord võivad äriprotsessid tunduda tavapäraseks, kuid tegelikult on need muudetud vastaste eesmärkide saavutamiseks. Need tehnikad võivad olla suunatud vastase lõppeesmärgi saavutamisele või konfidentsiaalsuse rikkumise varjamisele. [19]

2.2. HÄKKERI PROFIIL

Selle stsenaariumi korral kasutab musta mütsi häkker pahavara, mis krüpteerib failid ja palub nende dekrüpteerimise eest maksta.



Joonis 17. Pahavara allikas

Joonisel 17. on näidatud välja pahavara allika leht [20]

Sellist mõjutaktikat MITRE ATT&CK® andmebaasis nimetatakse "mõju jaoks krüpteeritud andmeteks", mis on:

Sissetungijad võivad krüpteerida andmeid sihtsüsteemides või mitmetes võrgusüsteemides, et katkestada juurdepääs süsteemile ja võrguressurssidele. Nad võivad püüda muuta salvestatud andmed ligipääsmatuks, krüpteerides faile või andmeid nii kohalikel kui ka kaugdraavidel ja blokeerides juurdepääsu dekrüpteerimisvõtmele. Seda tehakse mõnikord selleks, et saada ohvrilt rahalist hüvitist dekrüpteerimisvõtme eest või teha andmed pöördumatult kättesaamatuks juhtudel, kui võtit ei ole salvestatud ega edastatud.[21]

2.3. HÄKKERITE tegevus stsenaarium

Häkker kasutab pahavara sisestamiseks avaliku " User Execution: Malicious File " tehnikat.

MITRE ATT&CK® andmebaas kirjeldab tehnikat järgmiselt:

Vastane võib tugineda sellele, et kasutaja avab pahavara sisaldava faili, et saavutada täitmist. Kasutajaid võidakse mõjutada sotsiaalse inseneritöö abil, et nad avaksid faili, mis viib koodi täitmiseni. See kasutaja tegevus tavaliselt märgatakse pärast nokitsemist kinnitatud spämmi järelkäitumisena. [22]

Kasutaja laadis veebisaidilt alla piraatrakenduse ja käivitas selle.

PAHATAHTLIKU MÕJU JÄLGEDE LEIDMISEKS

Pahavara käivitamise järel käivitage USB-mälupulga abil RAM-i dumpimise tarkvara, valides dumpi salvestamise tee mälupulka.

Pärast seda saab RAM-i dumpi analüüsida erinevate RAM-i dumpide analüüsitarkvara funktsioonide abil.

3. MÄLUPILTI LOOMINE JA ANALÜÜSEERIMINE

3.1. MÄLUPILT

Mälupilt nimetatakse failiks, kus salvestatakse ühe protsessi, tuuma või kogu operatsioonisüsteemi RAM-i sisu. See võib sisaldada ka täiendavat teavet programmi või süsteemi oleku kohta.

Uurimise eesmärgil loome täieliku RAM-i dumpi.

Dump on sama mahuga kui RAM.

3.2. RAM-pildi loomise rakenduste analüüs ja võrdlus

Mälupilt loomisel kasutatakse järgmist tarkvara:

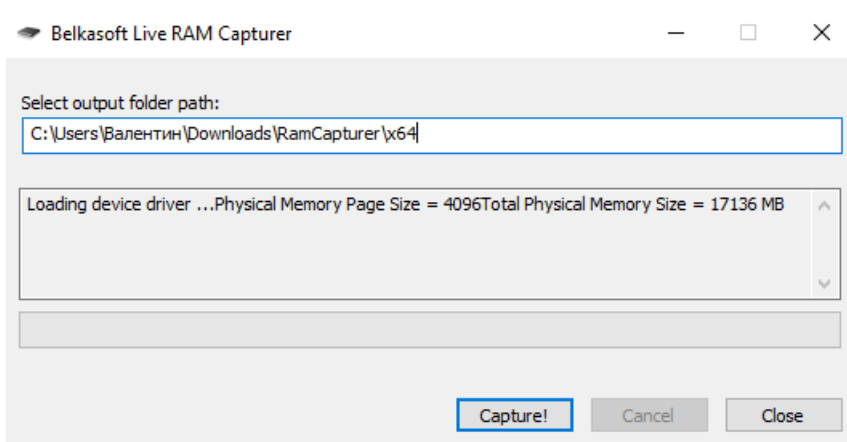
1. Belkasoft RAM Capturer
2. FTK Imager
3. WinPmem
4. Magnet RAM Capture

Rakendus	Peamised omadused	Kättesaadavus	Operatsioonisüsteemi tugi
Belkasoft RAM Capturer	Saab võtta andmeid RAM-ist ja salvestada need faili	Tasuta	XP, Vista, Windows 7, 8, 10
FTK Imager	Tööriist ketta- ja RAM-andmete kogumiseks, analüüsimiseks ja eelvaateks	Tasuta	Windows 10, Linux
WinPmem	Utiliit andmete kogumiseks RAM-ist Windowsi süsteemides	Tasuta	Windows 10, Windows 7, 8
Magnet RAM Capture	Tööriist RAM-ist andmete kogumiseks digitaalsel tasandil	Tasuta	XP, Vista, Windows 7, 8, 10

3.3. MÄLUPILDI LOOMINE

Mälu dumpide loomiseks on vaja USB-mälupulka, kuna tarkvara tuleb avada teise ketta kaudu, vastasel juhul käivitab operatsioonisüsteem väljalülita ja taaskäivitab süsteemi.

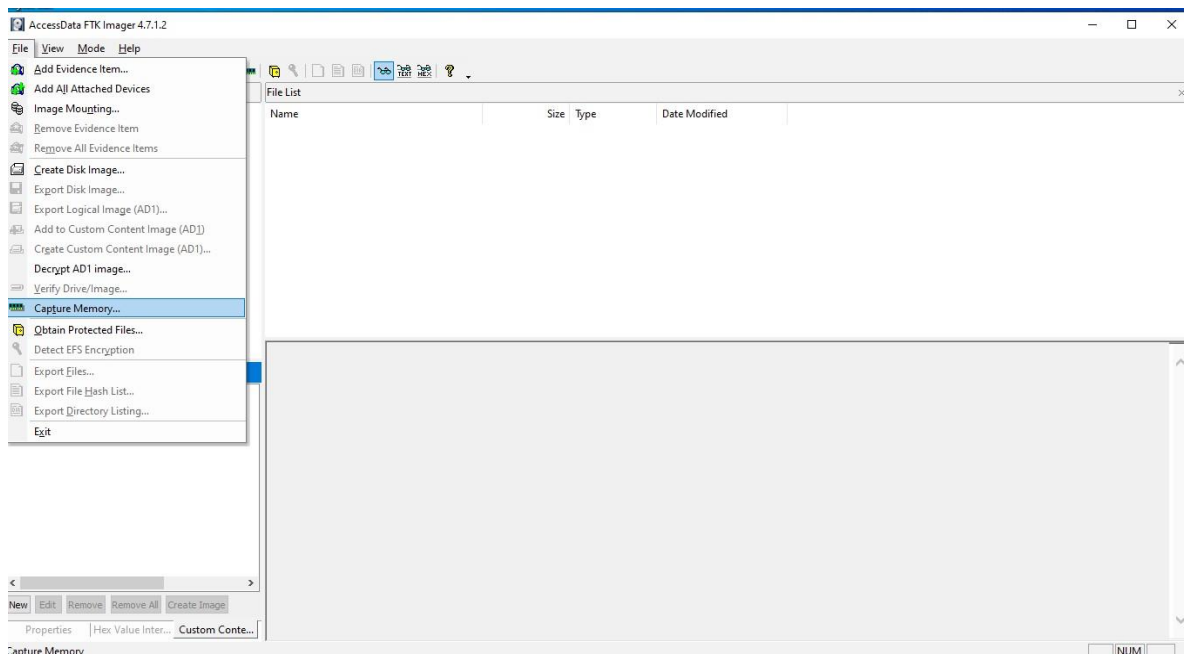
Seejärel tuleb tarkvara installida USB-mälupulgale ja käivitada mälupulgalt mälu kinni püüdmiseks ja dumpi loomiseks.



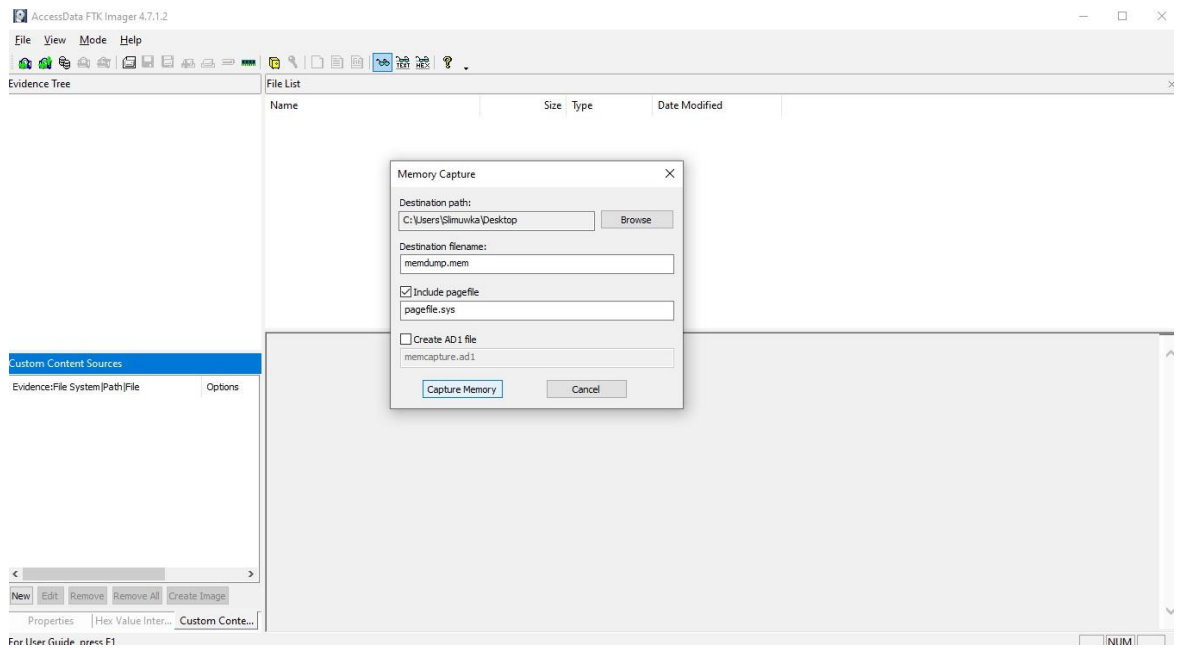
Belkasoft RAM Capturer

Joonis 18. Mälupildi loomine abiga Belkasoft RAM Capturer

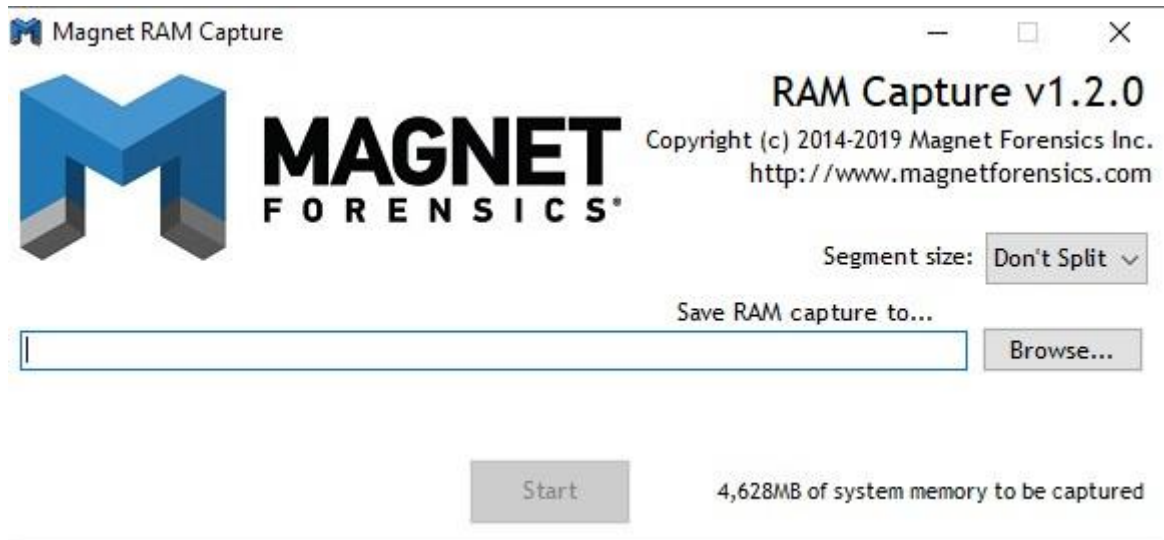
AccessData FTK Imager



Joonis 19. Mälupildi loomine abiga AccessData FTK Imager



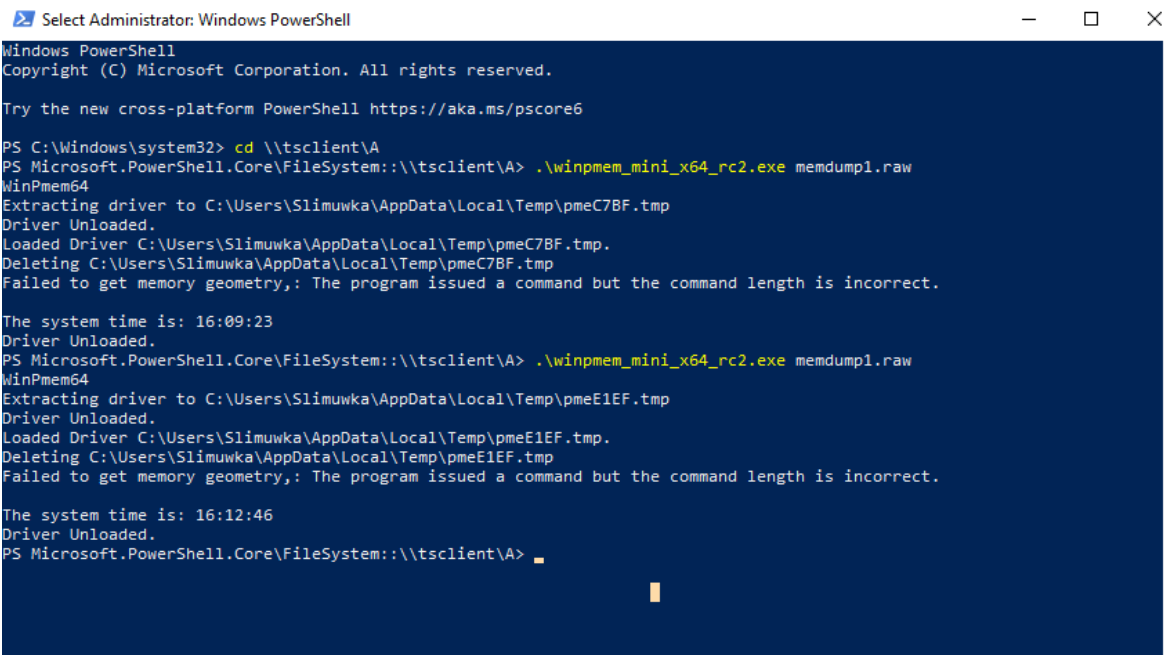
Joonis 20. Mälupildi loomine abiga AccessData FTK Imager
Magnet RAM Capture mälupiltide loomiseks



Joonis 21. Mälupildi loomine abiga Magnet RAM Capture
Tuleb valida koht, kuhu mälupilt jääb ja vajutada Start.

WinPmem

Mälupildi loomine nurjus



```
Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

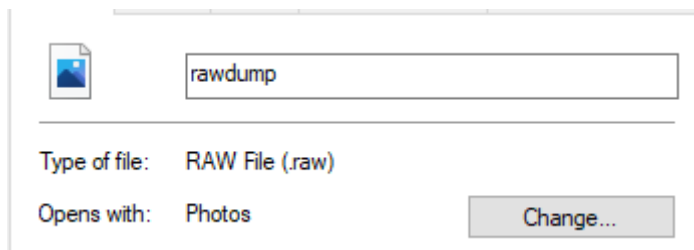
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd \\tsclient\A
PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\A> .\winpmem_mini_x64_rc2.exe memdump1.raw
WinPmem64
Extracting driver to C:\Users\Slimuwka\AppData\Local\Temp\pmeC7BF.tmp
Driver Unloaded.
Loaded Driver C:\Users\Slimuwka\AppData\Local\Temp\pmeC7BF.tmp.
Deleting C:\Users\Slimuwka\AppData\Local\Temp\pmeC7BF.tmp
Failed to get memory geometry, : The program issued a command but the command length is incorrect.

The system time is: 16:09:23
Driver Unloaded.
PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\A> .\winpmem_mini_x64_rc2.exe memdump1.raw
WinPmem64
Extracting driver to C:\Users\Slimuwka\AppData\Local\Temp\pmeE1EF.tmp
Driver Unloaded.
Loaded Driver C:\Users\Slimuwka\AppData\Local\Temp\pmeE1EF.tmp.
Deleting C:\Users\Slimuwka\AppData\Local\Temp\pmeE1EF.tmp
Failed to get memory geometry, : The program issued a command but the command length is incorrect.

The system time is: 16:12:46
Driver Unloaded.
PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\A> █
```

Joonis 22. Mälupildi loomine abiga WinPmem



Joonis 23. .raw laienduse Mälupilt



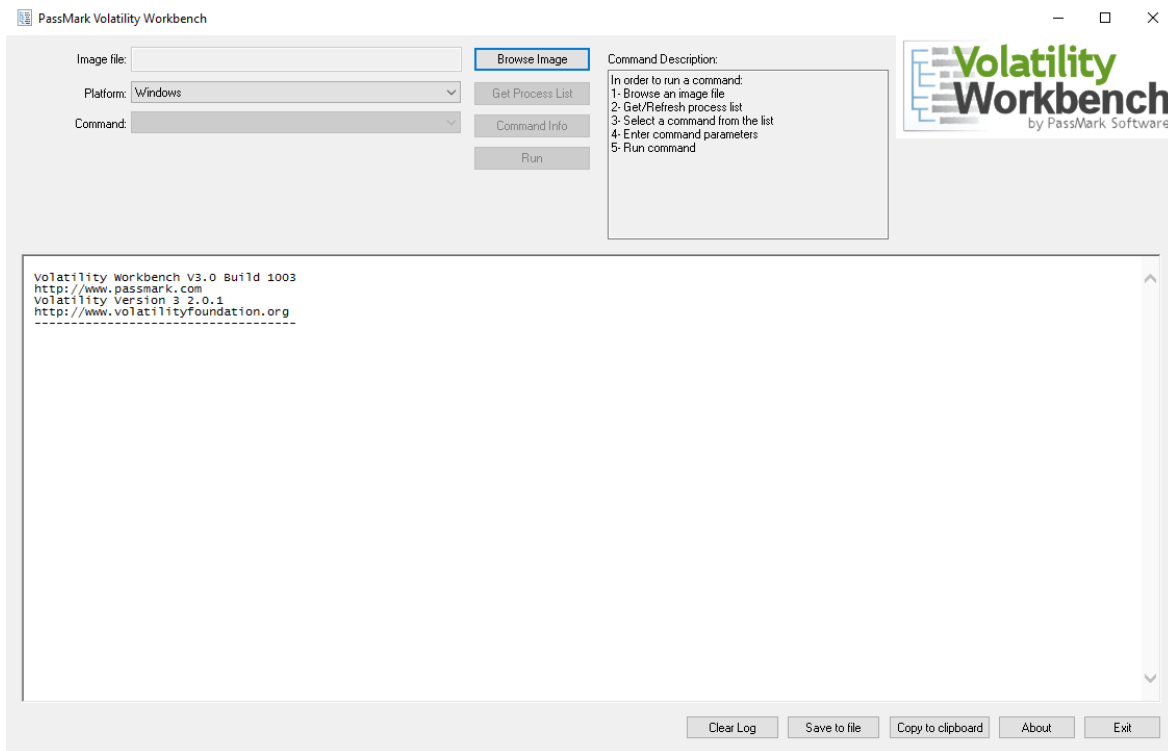
Joonis 24. .mem laienduse Mälupilt

Selle tarkvara abil on võimalik saada erinevaid laiendusi nagu .mem ja .raw

Kõige parem oli luua RAM- mälupilt "AccessData FTK Imager" abil.
Seetõttu kasutatakse edaspidi seda tarkvara mälupiltide loomiseks.

3.4. MÄLUPILDI ANALÜÜSIMINE

Mälupilti analüüsimiseks kasutatakse tarkvara «VolatilityWorkbench».



Joonis 25. «VolatilityWorkbench» tarkvara.

Kui klõpsate nuppu Browse Image, saate valida analüüsimiseks mälupilt.

Samuti on võimalik valida platvorm, kus loodi mälupilt ja erinevad käsud analüüsimiseks (Windows, Linux, Mac).

PassMark Volatility Workbench


Image file: E:\vmlfilp.mem Browse Image

Platform: Windows Refresh Process List

Command: windows.pslist.PsList Command Info

Command parameters:
 Display physical offsets
 Process ID Run

Command Description:
 Lists the processes present in a particular windows memory image



```

10600 1968 hkcmd.exe 0x81026c3e70c0 1 - 2 False 2023-05-17 22:26:02.000000 N/A Disabled
7260 1968 igfxpers.exe 0x81025da020c0 2 - 2 False 2023-05-17 22:26:02.000000 N/A Disabled
8800 888 RuntimeBroker.exe 0x8102676fa300 1 - 2 False 2023-05-17 22:26:03.000000 N/A Disabled
7852 1968 NvBackend.exe 0x8102716e80c0 6 - 2 True 2023-05-17 22:26:03.000000 N/A Disabled
6636 4864 LogonUI.exe 0x810268697080 0 - 2 False 2023-05-17 22:26:04.000000 2023-05-17 22:26:45.000000 Disabled
8256 888 Cortana.exe 0x81026b0ce080 16 - 2 False 2023-05-17 22:26:06.000000 N/A Disabled
7488 888 RuntimeBroker.exe 0x8102683be080 1 - 2 False 2023-05-17 22:26:08.000000 N/A Disabled
12500 668 svchost.exe 0x81026d6aa080 15 - 2 False 2023-05-17 22:26:09.000000 N/A Disabled
9024 888 LockApp.exe 0x81025da722c0 14 - 2 False 2023-05-17 22:26:38.000000 N/A Disabled
12132 888 RuntimeBroker.exe 0x8102644c6080 12 - 2 False 2023-05-17 22:26:39.000000 N/A Disabled
2212 888 ApplicationFrameHost.exe 0x81025db130c0 13 - 2 False 2023-05-17 22:27:01.000000 N/A Disabled
2732 888 ShellExperienceHost.exe 0x81025dfec080 13 - 2 False 2023-05-17 22:27:55.000000 N/A Disabled
6572 888 RuntimeBroker.exe 0x8102670e5080 2 - 2 False 2023-05-17 22:27:56.000000 N/A Disabled
12412 9136 Firefox.exe 0x810267a95080 0 - 2 True 2023-05-17 22:28:54.000000 2023-05-17 22:29:04.000000 Disabled
2260 4916 MusNotificationIcon.exe 0x8102671c8080 3 - 2 False 2023-05-17 22:29:03.000000 N/A Disabled
4396 668 svchost.exe 0x810267f56300 3 - 0 False 2023-05-17 22:29:29.000000 N/A Disabled
6400 5136 Dell.TechHub.1.exe 0x8102673d10c0 20 - 2 False 2023-05-17 22:30:14.000000 N/A Disabled
6272 1968 Zsm.exe 0x81026c0f0080 2 - 2 False 2023-05-17 22:31:04.000000 N/A Disabled
9080 668 WUDFHost.exe 0x81025dbc0f00 5 - 0 False 2023-05-17 22:32:39.000000 N/A Disabled
6868 888 smartscreen.exe 0x810263448080 7 - 2 False 2023-05-17 22:41:34.000000 N/A Disabled
12228 668 svchost.exe 0x810263440080 4 - 0 False 2023-05-17 22:43:00.000000 N/A Disabled
9488 888 SystemSettings.exe 0x81025fcaf300 24 - 2 False 2023-05-17 22:43:11.000000 N/A Disabled
10828 888 TextInputHost.exe 0x8102670dc080 11 - 2 False 2023-05-17 22:43:13.000000 N/A Disabled
2440 668 svchost.exe 0x810263021080 5 - 0 False 2023-05-17 22:44:11.000000 N/A Disabled
6064 1968 Zsm.exe 0x81026f0d0080 6 - 2 False 2023-05-17 22:48:52.000000 N/A Disabled
664 11444 fltwppor.exe 0x8102679c7080 7 - 2 True 2023-05-17 22:49:03.000000 N/A Disabled
7608 888 SecHealthUI.exe 0x810267d9080 32 - 2 False 2023-05-17 22:50:03.000000 N/A Disabled
584 888 SecurityHealth.exe 0x810264b2f080 19 - 2 False 2023-05-17 22:50:04.000000 N/A Disabled
7132 1968 vlc.exe 0x81026d494080 0 - 2 True 2023-05-17 22:50:21.000000 2023-05-17 22:50:25.000000 Disabled
11044 3628 firefox.exe 0x81025db1e300 0 - 2 True 2023-05-17 22:50:27.000000 2023-05-17 22:50:33.000000 Disabled
11716 1968 FTK Imager.exe 0x81025dbdd1080 21 - 2 False 2023-05-17 22:50:54.000000 N/A Disabled

Time Stamp: Thu May 18 02:14:07 2023
***** End of command output *****

```

Clear Log Save to file Copy to clipboard About Exit

Joonis 26. Mälupildi analüüsimine abiga «VolatilityWorkbench».

Käsuga windows.pslist.PsList käsku avastati kahtlane protsess ja pärast nime kontrollimist Googlis võib järeldada, et see on pahatahtlik protsess.



fijtweorc.exe



Все Картинки Видео Новости Ещё

Инструменты

Результатов: примерно 3 (0,24 сек.)

joesandbox.com
<https://www.joesandbox.com/analysis/html>

Automated Malware Analysis Report for SO# GOSUSNH1637860.exe

Behavior: SO# GOSUSNH1637860.exe, pid: 2448; **fijtweorc.exe**, pid: 5848; **fijtweorc.exe**, pid: 1144. Disassembly. Disassembly; SO# GOSUSNH1637860.exe, ...

drweb.com
<https://vms.drweb.com/virus> · Перевести эту страницу

Trojan.PWS.Siggen3.27004 — Dr.Web Malware description library

Malicious functions injects code into the following user processes: **fijtweorc.exe**. Searches for registry branches where third party applications store ...

abuse.ch
<https://bazaar.abuse.ch/sam...> · Перевести эту страницу

MalwareBazaar Database - Abuse.ch

27 фев. 2023 г. — File size: 323'439 bytes. First seen: 2023-02-27 20:42:42 UTC. Last seen: 2023-02-27 22:27:55 UTC. File type: Executable **exe**.

Joonis 27. Mälupildi analüsimine abiga «VolatilityWorkbench».

4. TÖÖ TULEMUSED

Töö eesmärk oli uurida, mis on digitaalne kriminalistika, uurida häkkimistehnikaid ja -meetodeid, luua häkkeri stsenaarium. Uurida ja analüüsida andmemälu digitaalse kohtuekspertiisi abil ning otsida sissetungimise jälgi operatsioonisüsteemi Windows 10 kasutamisel. Uuriti erinevaid vahendeid mäludumpi tegemiseks. Uuritakse erinevaid rünnakute tehnikaid ja meetodeid ning nende mõju süsteemile. Süsteem oli nakatunud ja pärast analüüsi leiti mälupildilt nakkuse jälgi.

Õppimise ja töötamise protsessis õppis autor palju uusi asju infosüsteemide turvalisuse ja nende kaitse valdkonnas. Töö käigus oli autoril probleeme mälukaardi loomisega, sest kohe ei olnud võimalik välja selgitada, kuidas mälupilti saamiseks õigesti tegutseda, samuti oli probleem pahavara vastuvõtmisega. Kuna selgus, et pahavara hankimine ja selle toimimise mõistmine ning seejärel õigesti kasutamine stsenaariumis ei ole nii lihtne.

KOKKUVÕTE

Valentin Mihhaiski lõputöö "Digitaalse kohtuekspertiisi kasutamine sissetungijate jälgede otsimiseks" keskendub küberkuritegude jälgede otsimisele mälu dumpi analüüsi abil.

Töö esimeses osas uuris autor erinevaid häkkereid, nende motivatsioone ning kuidas arvutimälu võib aidata küberkuritegude jälgede leidmisel. Samuti analüüsis autor IT-turvalisust, et mõista, kuidas end kaitsta küberkuritegude eest, millised ohud võivad operatsioonisüsteemile tekkida, ja milliseid IT-haavatavusi võib küberkurjategija kasutada IT-rünnakute sooritamiseks ning millist kahju võib selline rünnak tekitada.

Töö teises osas uuris autor ülemaailmselt kättesaadavat teadmiste baasi küberkurjategijate taktikate ja meetodite kohta, et selle põhjal välja mõelda rünnaku ja süsteemi nakatumise stsenaarium ning proovida pärast nakatumist avastada selle küberkuriteo jälgi. Autor näitas ka välja mõeldud häkkeri profiili ja tema tegevusi, millist pahavara ta kasutab ning millise tehnikaga ta nakatab infosüsteemi pahavaraga. Seejärel selgitas autor, kuidas saab avastada küberkuriteo jälgi, luues ja analüüsides operatiivmälu dumpi.

Töö kolmandas osas vaatles autor erinevaid rakendusi, mis suudavad luua mälu dumpi, võrdles neid mitme kriteeriumi järgi ja lõi nakatunud infosüsteemi mälu dumpi. Autor näitas ka programmi mugavaks mälu dumpi analüüsiks. Lõpuks kasutas autor mälu dumpi analüüsi programmi, et edukalt avastada pahatahtlik protsess ja saada selle kohta üksikasjalikku teavet, näiteks millal see käivitati.

Kokkuvõttes näitas autor, et kõik töö eesmärgid on saavutatud.

SUMMARY

Valentin Mihhaiski's thesis "Using Digital Forensics for Tracing Intruders Traces" is dedicated to searching for traces of cybercrimes through the analysis of memory dumps.

In the first part of the thesis, the author explored various hackers, their motivations, and how computer memory can assist in finding traces of cybercrimes. The author also analyzed IT security to understand how to defend against cybercrimes, the threats that an operating system may face, and the IT vulnerabilities that a cybercriminal could exploit for IT attacks, and the potential damage such an attack could cause.

In the second part of the thesis, the author studied globally available knowledge about the tactics and methods of cybercriminals to devise an attack and system infection scenario based on it. The author tried to detect traces of this cybercrime after infection. The author also presented a fictional hacker profile and their actions, the malware they use, and the technique they use to infect the information system with malware. The author then explained how to detect traces of cybercrime by creating and analyzing a dump of the random-access memory (RAM).

In the third part of the thesis, the author examined various applications capable of creating a memory dump, compared them based on several criteria, and created a memory dump of an infected information system. The author also presented a program for convenient memory dump analysis. Ultimately, using the memory dump analysis program, the author successfully detected a malicious process and obtained detailed information about it, such as when it was launched.

In conclusion, the author demonstrated that all the goals of the thesis were achieved.

KASUTATUD KIRJANDUSE LOETELU

1. Practical Memory Forensics (2022)

2. Understanding vulnerabilities

<https://www.ncsc.gov.uk/information/understanding-vulnerabilities>

3. IT Security Vulnerability vs Threat vs Risk: What are the Differences?

<https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/>

4. What is a hacker?

<https://us.norton.com/blog/emerging-threats/what-is-a-hacker>

5. MITRE ATTACK

<https://attack.mitre.org/>

6. MITRE ATTACK- Reconnaissance

<https://attack.mitre.org/tactics/TA0043/>

7. MITRE ATTACK- Resource Development

<https://attack.mitre.org/tactics/TA0042/>

8. MITRE ATTACK- Initial Access

<https://attack.mitre.org/tactics/TA0001/>

9. MITRE ATTACK- Execution

<https://attack.mitre.org/tactics/TA0002/>

10. [Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®](#)

11. [Privilege Escalation, Tactic TA0004 - Enterprise | MITRE ATT&CK®](#)

12. [Defense Evasion, Tactic TA0005 - Enterprise | MITRE ATT&CK®](#)

13. [Credential Access, Tactic TA0006 - Enterprise | MITRE ATT&CK®](#)

14. [Discovery, Tactic TA0007 - Enterprise | MITRE ATT&CK®](#)

15. [Lateral Movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®](#)

16. [Collection, Tactic TA0009 - Enterprise | MITRE ATT&CK®](#)

17. [Command and Control, Tactic TA0011 - Enterprise | MITRE ATT&CK®](#)

18. [Exfiltration, Tactic TA0010 - Enterprise | MITRE ATT&CK®](#)
19. [Impact, Tactic TA0040 - Enterprise | MITRE ATT&CK®](#)
20. <https://malshare.com/>
21. [Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®](#)
22. [User Execution: Malicious File, Sub-technique T1204.002 - Enterprise | MITRE ATT&CK®](#)