Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS
KIBERNETINIO INCIDENTO TYRIMUI BŪTINOS INFORMACIJOS SURINKIMAS IR IŠSAUGOJIMAS

2024 m. sausio 29 d.

Nacionalinis kibernetinio saugumo centras (toliau – NKSC) nacionaliniu lygmeniu stebėdamas kibernetinius incidentus ir atlikdamas jų tyrimus pastebi, kad Kibernetinio saugumo subjektai (toliau – Subjektai) valdant kibernetinius incidentus vis dar nepakankamai dėmesio skiria jų tyrimams ir tyrimams būtinų įrodymų išsaugojimui. Įvykus kibernetiniam incidentui, subjektai įprastai siekia kaip galima greičiau jį suvaldyti t. y. pašalinti incidento padarinius. Priklausomai nuo kibernetinio incidento tipo ir poveikio, kartais tenka atstatinėti ir sistemų veikimą: paleisti iš naujo (angl. *restart*) tarnybinės stotis, pasinaudoti duomenų atsarginėmis kopijomis, įdiegti papildomą programinę įrangą ar saugumo sprendimus. Atstačius sistemų veikimą ir toliau atliekant kibernetinio incidento tyrimą, neretai susiduriama su problema, kad tyrimui reikalinga informacija būna prarasta. Pavyzdžiui, paleidus iš naujo tarnybinę stotį yra prarandama visa operatyviojoje atmintyje esanti informacija.

Neatlikus išsamaus kibernetinio incidento **tyrimo** ir neišsiaiškinus incidento atsiradimo priežasčių bei pasekmių, išlieka didelė tikimybė, kad: **incidentas pasikartos**, **nebus identifikuotos visos pažeistos sistemos / įrenginiai, nenustatyti piktavalių atlikti veiksmai** ir pan.

Šiame informaciniame biuletenyje priminsime kokius veiksmus reikėtų atlikti siekiant maksimaliai sumažinti informacijos, reikalingos kibernetinio incidento tyrimui, praradimo tikimybę. Pateiksime įrankius ar komandas, kurių pagalba galima greitai ir paprastai surinkti pirminę informaciją apie ***„Windows“*** šeimos operacinėse sistemose vykstančius procesus, naudotojus / grupes, tinklo sujungimus ir pan. Pažymime, kad atsižvelgiant į kibernetinio incidento

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

tipą ir poveikį, visada reikia įvertinti kokius veiksmus reikėtų atlikti pirmiausiai: sustabdyti failus šifruojančio žalingo programinio kodo veikimą ar sukurti operatyviosios atminties atvaizdą.

Operatyviosios atminties atvaizdo sukūrimas

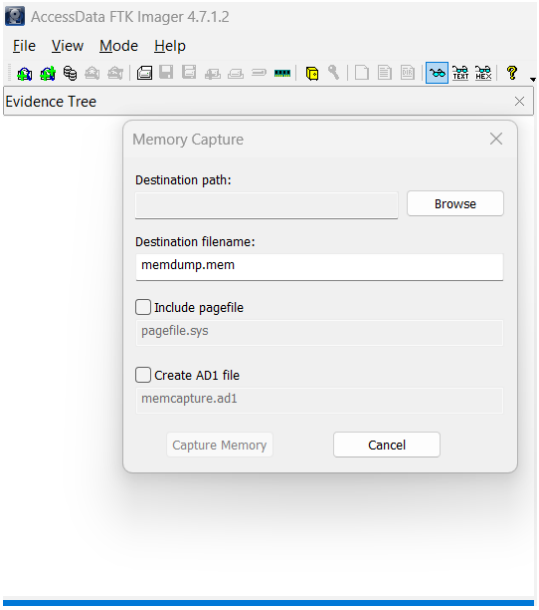
Operatyviosios atminties analizė užima svarbią vietą kibernetinio incidento tyrime. Siekiant apeiti kibernetinio saugumo priemones, pasislėpti ar paslėpti įkalčius, piktavaliai stengiasi žalingą programinį kodą įdiegti tiesiai į įrenginio operatyviąją atmintį. Dažniausiai operatyviojoje atmintyje žalingas programinis kodas saugomas neužkoduotas ar neužšifruotas. Aptikus žalingą programinį kodą ir jį išanalizavus pavyksta nustatyti kokius veiksmus atliko piktavaliai ar kokį tikslą jie norėjo pasiekti.

Siekiant neprarasti kibernetinio incidento tyrimui svarbios informacijos, kuri gali būti išlikusi įrenginio operatyviojoje atmintyje, rekomenduojame pirmiausiai (**neatliekant jokių kitų veiksmų**) sukurti ir išsaugoti operatyviosios atminties atvaizdą. Operatyviosios atminties atvaizdas gali būti išsaugotas skirtingais formatais: ***„aff4“***, ***„raw“*** ar ***„dmp“***. Rekomenduojame naudoti ***„raw“*** formatą.

Operatyviosios atminties atvaizdą galima sukurti pasinaudojus nemokama trečiųjų šalių programine įranga, pavyzdžiui:

- ***„WinPmem“***, daugiau informacijos https://github.com/Velocidex/WinPmem;
- ***„FTK Imager“***, daugiau informacijos https://www.exterro.com/ftk-imager;
- ***„MAGNET DumpIt“***, daugiau informacijos https://www.magnetforensics.com/resources/magnet-dumpit-for-windows/.

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt



1 pav. ***„FTK Imager“*** programinės įrangos langas

Naudojantis virtualizacijos platformomis, operatyviosios atminties atvaizdą galima sukurti pačių platformų priemonėmis. Detalesnės informacijos reikėtų ieškoti virtualizacijos platformos gamintojo oficialioje dokumentacijoje, pavyzdžiui:

- https://techcommunity.microsoft.com/t5/ask-the-performance-team/difficulty-generating-a-memory-dump/ba-p/2351370;
- https://kb.vmware.com/s/article/2003941.

Disko atvaizdo sukūrimas

Įvykus kibernetiniam incidentui neretai siekiama kaip galima greičiau atstatyti darbo ar tarnybinės stoties veikimą, o tik po to pagalvojama apie detalesnį tyrimą. Siekiant išsiaiškinti kibernetinio incidento priežastį ir sumažinti tikimybę tokių incidentų pasikartojimui, visada reikėtų atlikti jo tyrimą.

Norint išsaugoti kuo daugiau informacijos, susijusios su kibernetiniu incidentu, visada rekomenduojame sukurti ir išsaugoti įrenginio „kietojo“ disko atvaizdą (angl. *image*). Toks

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

būdas laiko atžvilgiu nėra efektyvus, tačiau minimizuoja informacijos (įkalčių / artefaktų) praradimą ar sugadinimą. Reikėtų pažymėti, kad disko atvaizdai užima daug vietos, tad reikėtu pasirūpinti vieta / disku, kur bus saugomas disko atvaizdas. Disko atvaizdas gali būti išsaugotas skirtingais formatais: „***E01“***, ***„raw“, „smart“*** ar ***„aff“***. Rekomenduojame naudoti ***„E01“*** ar ***„raw“*** formatus.

Disko atvaizdą galima sukurti pasinaudojus nemokama trečiųjų šalių programine įranga, pavyzdžiui:

- ***„FTK Imager“***, daugiau informacijos https://www.exterro.com/ftk-imager;
- ***„WinPE“***, daugiau informacijos https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/download-winpe--windows-pe?view.

Naudojantis virtualizacijos platformomis, daugeliu atveju, atskirai disko atvaizdo kurti nereikia, kadangi virtualus diskas saugomas kaip failas. Virtualaus disko formatas priklauso nuo virtualizacijos platformos gamintojo. Dažniausiai naudojamų virtualių diskų formatai: ***„vmdk“***, ***„vhd“***, ***„vhdx“*** ar ***„vdi“***.

Pirminės informacijos surinkimas

Kaip jau buvo minėta, įvykus kibernetiniam incidentui, labai svarbu surinkti, išsaugoti ir nesunaikinti informacijos, reikalingos kibernetinio incidento tyrimui. Kartais sukūrus ir išsaugojus įrenginio operatyviosios atminties atvaizdą, kibernetinio incidento tyrimui ar situacijos suvaldymui kyla būtinybė surinkti pirminę informaciją veikiančioje (angl. *live*) sistemoje.

Pirmiausiai rekomenduojame patikrinti:

- tinklo sujungimus (angl. *network connections*), tinklo prievadus;
- rinkmenų mainus (angl. *file sharing*);
- atidarytas sesijas (angl. *open sessions*);
- ***„NetBios“*** naudojimą;
- ***„arp“*** lentelę ir ***„dns“*** nustatymus;
- veikiančius procesus;

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

- įdiegtus servisus;
- veikiančius procesus ir naudojamus ***„dll“*** failus;
- sisteminius uždavinius (angl. *scheduled tasks*);
- programinę įrangą, kuri sukonfigūruota startuoti operacinės sistemos startavimo metu arba (naudotojo) prisijungimo metu;
- naudotojus, jų teises ir grupes;
- failus esančius ***„C:\temp“***, ***„C:\ProgramData“***, ***„C:\$Recycle.Bin“*** ar ***„C:\Users\UserName\AppData“***;
- įvykių žurnalus (angl. *logs*).

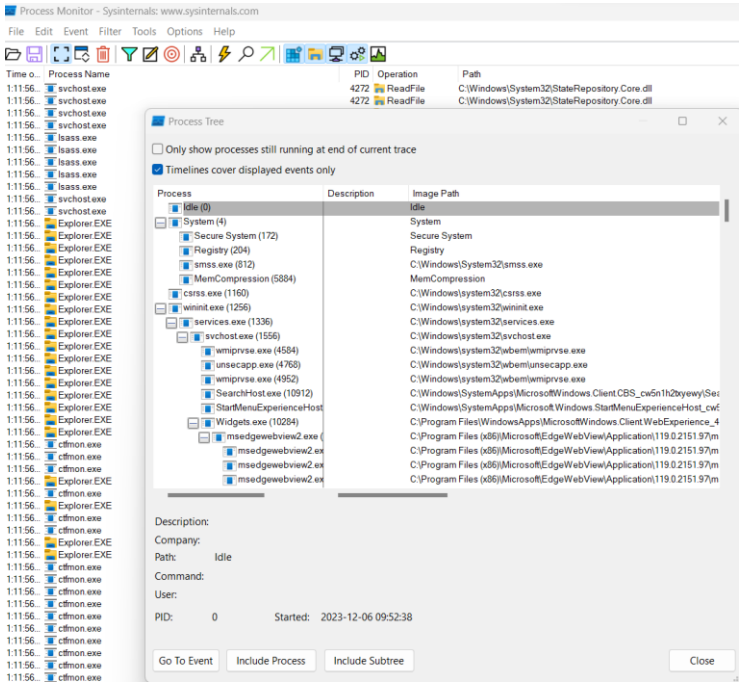
„Windows“ operacinėse sistemose pirminės informacijos surinkimui galima naudoti ***„Sysinternals Suite“***[1] programinę įrangą:

- ***„PsLoggedOn“*** – padeda identifikuoti tiek lokaliai, tiek nuotoliniu būdu (angl. *remotely*) prisijungusius (angl. *logged on*) naudotojus;
- ***„PsFile“*** – pateikia informaciją apie nuotoliniu būdu atidarytus failus, taip pat suteikia galimybę juos uždaryti;
- ***„PsService“*** – pateikia informaciją ir leidžia valdyti operacinėje sistemoje įdiegtus servisus. Leidžia nuotoliniu būdu prisijungti prie kitų sistemų/įrenginių;
- ***„TCPView“*** – pateikia informaciją apie tinklo sujungimus (***„tcp“*** ir ***„udp“*** protokolais);
- ***„Process Monitor“*** – realiu laiku pateikia informaciją apie operacinėje sistemoje veikiančius procesus, failus, registrus ir pan.;
- ***„Autoruns“*** – pateikia informaciją apie programinę įrangą, kuri sukonfigūruota startuoti operacinės sistemos startavimo metu arba (naudotojo) prisijungimo metu;
- ***„ListDLLs“*** – pateikia informaciją apie ***„dll“*** formato failus, kurie naudojami procesų veikime (angl. *loaded into processes*);

[1] https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

- ***„Strings“*** – vykdomuosiuose ir objektų failuose ieško ***„UNICODE“*** / ***„ASCII“*** raktažodžius, kurių ilgis 3 ar daugiau ***„UNICODE“*** / ***„ASCII“*** simbolių.



2 pav. ***„Process Monitor“*** programinės įrangos langas

Daugiau informacijos apie ***„Sysinternals Suite“*** programinę įrangą ir jos galimybes – https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite. Atkreipiame Jūsų dėmesį, kad ***„Sysinternals Suite“*** programinė įranga netik leidžia gauti įvairią informaciją apie operacinėje sistemoje vykstančius procesus, bet ir leidžia išsaugoti gautus rezultatus tolimesnei kibernetinio incidento analizei.

Piktavaliai įvairiais būdais stengiasi operacinėje sistemoje paslėpti žalingos programinės įrangos veikimą naudojant įvairius metodus ar technikas. Tam tikrais atvejais (esant tokiam funkcionalumui), žalingas programinis kodas gali gebėti identifikuoti ***„Sysinternals Suite“*** programinės įrangos naudojimą / veikimą. Įtarus, kad operacinėje sistemoje veikia moderni kenkimo programinė įranga (angl. *advanced persistent threat*, *APT*), kaip jau buvo minėta, pirmiausiai reikėtų sukurti operatyviosios atminties atvaizdą. Tokiais atvejais, siekiant gauti daugiau informacijos apie operacinėje sistemoje vykstančius procesus, naudinga naudotis

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

„Windows“ integruotais (angl. *build in*) funkcionalumais: ***„WMIC“***, ***„PowerShell“*** ar ***„Command shell“***.

Žemiau esančiose lentelėse pateikti komandų pavyzdžiai, kurios gali būti naudojamos kasdienėje veikloje arba įvykus kibernetiniui incidentui. Pateiktas komandų sąrašas nėra baigtinis. Papildomą informaciją apie kiekvieną komandą ir jos *„raktus“* galima gauti prie komandos pridėjus simbolius ***„/?“***, pavyzdžiui ***„whoami /?“***.

1 lentelė. Komandų pavyzdžiai

Komanda	Komentaras
whoami /all	Gaunama informacija apie operacinėje sistemoje veikiančius / sukurtus naudotojus (angl. *users*), grupes ir teises
netstat –naob	Gaunama informacija apie aktyvius tinklo sujungimus, raktas ***„-n“*** parodo tinklo prievadus (numerius), raktai ***„-o“*** ir ***„-b“*** parodo proceso ***„id“*** ir paleidžiamojo failo (ar ***„dll“***) vardą
net view \\127.0.0.1	Gaunama informacija apie rinkmenų mainus (angl. *file sharing*)
net session	Gaunama informacija apie įeinančias ***„smb“*** sesijas
net use	Gaunama informacija apie išeinančias ***„smb“*** sesijas
net start	Gaunama informacija apie operacinėje sistemoje veikiančius servisus
net user	Gaunama informacija apie operacinėje sistemoje sukurtus / naudojamus naudotojus (angl. *users*) (lokalius)
net localgroup administrators	Gaunama informacija apie operacinės sistemos grupėje ***„Administrators“*** esančius naudotojus (angl. *users*)
nbtstat –S	Gaunama informacija apie ***„NetBios“*** sesijas ir jų statusą

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

tasklist	Gaunama informacija apie operacinėje sistemoje veikiančius procesus
tasklist /v	Gaunama detalesnė informacija apie operacinėje sistemoje veikiančius procesus
tasklist /svc	Gaunama informacija apie operacinėje sistemoje veikiančius procesus ir jų sąryšį su servisais
tasklist /m /fi "pid eq pid_num"	Gaunama detalesnė informacija apie nurodytą procesą (***„pid_num“*** – proceso PID numeris) ir naudojamus ***„dll“*** failus
services.msc	Gaunama informacija apie operacinėje sistemoje įdiegtus / veikiančius servisus (grafinė aplinka)
sc query |more	Gaunama detalesnė informaciją apie operacinėje sistemoje įdiegtus servisus
reg query "regkey"	Gaunama informacija apie specifinį operacinės sistemos registrą, pavyzdžiui, ***"reg query HKLM\Software\"***
lusrmgr.msc	Gaunama informacija apie operacinėje sistemoje sukurtus / naudojamus naudotojus (angl. *users*) ir grupes (angl. *groups*) (grafinė aplinka)
FOR /R C:\ %i in (*) do @if %~zi gtr 10000000 echo %i %~zi	Operacinėje sistemoje atliekama failu paieška, kurių dydis didesnis nei 10 MB
schtasks	Gaunama informacija apie operacinėje sistemoje sukurtus sisteminius uždavinius (angl. *scheduled tasks*)
arp –a	Gaunama ***„arp“*** lentelės (angl. *ARP table*) informacija
ipconfig /displaydns	Gaunama informacija apie visus operacinėje sistemoje išsaugotus (angl. *cached*) ***„DNS“*** įrašus

„WMIC“ (Windows Management Instrumentation Command) – komandinės eilutės įrankis leidžiantis pasiekti sistemos išteklius ir nustatymus, atlikti užklausas ir tvarkyti sistemos

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

informaciją bei atlikti įvairias administravimo užduotis. Žemiau pateiktas komandų sąrašas nėra baigtinis, daugiau informacijos apie ***„WMIC“*** rasite - https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmic.

2 lentelė. Komandų pavyzdžiai

Komanda	Komentaras
wmic OS GET CAPTION,VERSION	Gaunama informacija apie operacinę sistemą ir jos versiją
wmic process list brief	Gaunama informacija apie operacinėje sistemoje veikiančius procesus
wmic process list full	Gaunama detalesnė informacija apie operacinėje sistemoje veikiančius procesus
wmic process get name,parentprocessid,workingsetsize	Gaunama informacija apie operacinėje sistemoje veikiančius procesus, nurodžius

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

	konkrečius laukus, pavyzdžiui, ***„name“***, ***„parentprocessid“***, ***„workingsetsize“***
wmic process where processid= pid_num get commandline	Gaunama detalesnė informacija apie konkretų (***„pid_num“*** – nurodomas proceso PID numeris) operacinėje sistemoje veikiantį procesą
wmic product get name,version,vendor	Gaunama informacija apie operacinėje sistemoje įdiegtą programinę įrangą
wmic startup list full	Gaunama informacija apie programinę įrangą, kuri sukonfigūruota startuoti operacinės sistemos startavimo metu arba (naudotojo) prisijungimo metu

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

wmic service list brief	Gaunama informacija apie operacinėje sistemoje įdiegtus servisus (pavadinimas, id, būsena ir pan.)
wmic product get name,version	Gaunama informacija apie operacinėje sistemoje įdiegtą programinė įrangą
wmic useraccount list full	Gaunama informacija apie naudotojus ir grupes
wmic nic get AdapterType, Name, Installed, MACAddress, PowerManagementSupported, Speed	Gaunama informacija apie tinklo prievadus, jų ***„MAC“*** adresus ir pan.
wmic nicconfig get caption,IPAddress,IPSubnet,DefaultIPGateway,DNSServerSearchOrder	Gaunama informacija apie tinklo sąsajų IP adresus, tinklo kaukes, ***„DNS“*** adresus ir pan.

„PowerShell“ yra automatizavimo platforma bei scenarijų rašymo kalba, skirta valdyti ***„Windows“*** šeimos operacines sistemas. Ji leidžia manipuliuoti ir valdyti duomenis kaip

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

objektus, turi integruotas komandas (angl. *cmdlets*), palaiko nuotolinio valdymo galimybes, palaiko .NET ir COM pagrindu veikiančius objektus. Žemiau pateiktas komandų sąrašas nėra baigtinis, daugiau informacijos apie „Powershell“ galimybės rasite - https://learn.microsoft.com/en-us/powershell/?view=powershell-7.4.

3 lentelė. Komandų pavyzdžiai

Komanda	Komentaras
query user	Gaunama informacija prisijungusius (angl. *logged on*) naudotojus;
Get-Process	Gaunama informacija apie operacinėje sistemoje veikiančius procesus
Get-Process process_name | Format-List *	Gaunama detalesnė informacija apie konkretų operacinėje sistemoje veikiantį procesą (***„process_name“ –*** nurodomas proceso vardas)
(Get-WmiObject win32_process -Filter ProcessId=pid_num -Property CommandLine).CommandLine	Gaunama detalesnė informacija apie konkretų operacinėje sistemoje veikiantį procesą (su paleidimo komandine eilute) (***„pid_num“*** – proceso PID numeris)
Get-WmiObject -Class Win32_Product	Gaunama informacija apie operacinėje sistemoje įdiegtą programinę įrangą
Get-CimInstance Win32_StartupCommand | Select-Object Name, command, Location, User | Format-List	Gaunama informacija apie programinę įrangą, kuri sukonfigūruota startuoti operacinės sistemos startavimo metu arba (naudotojo) prisijungimo metu
Get-Service	Gaunama informacija apie operacinėje sistemoje įdiegtus servisus (pavadinimas, id, būsena ir pan.)

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

Get-SmbSession	Gaunama informacija apie ***„NetBios“*** sesijas ir jų statusą
Get-WmiObject -Class Win32_UserAccount	Gaunama informacija apie naudotojus ir grupes (lokalius)
Get-NetTCPConnection	Gaunama informacija apie tinklo sujungimus (IP adresai, prievadai, statusas ir pan.)
Get-Process process_name | select -ExpandProperty modules | group -Property FileName | select name	Gaunama informacija apie ***„dll“*** failus, kurie naudojami procesų veikime (angl. *loaded into processes*). ***„process_name“*** nurodomas proceso pavadinimas.
Get-ChildItem -Path C:\ -Recurse -Include *.log	Atliekama ****.log*** formato failų paieška „C“ diske

Įvykių žurnalų surinkimas ir išsaugojimas

Viename iš informacinių biuletenių jau rašėme, kad labai svarbu tinkamai sukonfigūruoti auditavimo, įvykių žurnalų registravimo ir saugojimo funkcionalumą. Suprantama, kad tai atlikti reikėtų nelaukiant kada įvyks kibernetinis incidentas. Daugiau informacijos kaip tai atlikti rasite - https://www.nksc.lt/doc/biuleteniai/NKSC%20Informaciniu%20istekliu%20zurnaliniu%20irasu%20politika%20windows.pdf.

„Windows“ šeimos operacinėse sistemose (***„Windows Vista“*** ir naujesnės) įvykių žurnalai saugomi kataloge ***„C:\Windows\System32\winevt\Logs“***. Reikėtų paminėti, kad darbo ar tarnybinėse stotyse įdiegta papildoma programinė įranga, įskaitant ir saugumo priemones, gali kaupti atskirus įvykių žurnalus. Jų saugojimo vieta priklauso nuo konkrečios programinės įrangos, todėl reikėtų nepamiršti išsaugoti ir šių įvykių žurnalų.

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

Informacija apie operacinėje sistemoje vykstančius procesus ar jos konfigūraciją saugoma ne tik įvykių žurnaluose, bet ir tam tikruose failuose (duomenų bazėse):

- registrų (angl. *registry*) failai ***„SYSTEM“***, ***„SOFTWARE“***, ***„SAM“***, ***„SECURITY“*** ir kt. saugomi kataloge ***„C:\Windows\System32\config\“*** ir ***„NTUSER.dat“*** saugomas kataloge ***„C:\Users\<username>\“***. Failuose saugoma informacija apie operacinių sistemų, programinės įrangos ar naudotojų nustatymus, saugoma prisijungimo informacija, naudotojo atlikti veiksmai ir pan.;
- failas ***„UsrClass.dat“*** saugomas kataloge ***„C:\Users\<username>\AppData\Local\Microsoft\Windows\“***. Faile saugoma informacija apie konkretaus naudoto profilio konfigūraciją ir nustatymus;
- ***„.pf“*** formato failai. Saugomi kataloge ***„C:\Windows\Prefetch“***. Failuose saugoma informacija apie vykdomųjų failų paleidimą operacinėje sistemoje (paleidimo data, komandinė eilutė, naudojami ***„dll“*** failai ir pan.);
- failas ***„Amcache.hve“***. Saugomas kataloge ***„C:\Windows\AppCompat\Programs\“***. Faile saugoma informacija apie vykdomųjų failų paleidimą (suderinamumą) operacinėje sistemoje (paleidimo data, komandinė eilutė, naudojami ***„dll“*** failai ir pan.);
- failas ***„SRUDB.dat“***. Saugomas kataloge ***„C:\Windows\System32\sru\“***. Faile saugoma informacija apie resursų (procesoriaus, atminties, disko ar tinklo) ir programinės įrangos naudojimą;

Įsilaužus į įstaigos vidinį tinklą, piktavaliai stengiasi pasiekti kuo daugiau resursų, atlieka žvalgybą, pavyzdžiui skenuoja tinklo prievadus ar ieško pažeidžiamumų, kuriuos galėtų vėliau išnaudoti tolimesnėms atakoms. Svetainių / informacinių sistemų prieigos, el. pašto, tinklo įrangos (pavyzdžiui ***„NetFlow“***), ugniasienių ar saugumo priemonių įvykių žurnalai neretai leidžia gauti svarbios ir naudingos informacijos apie kibernetinį incidentą bei padeda identifikuoti pažeistas sistemas ar įrenginius.

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

Surinktos informacijos saugojimas ir perdavimas

Surinkus kibernetinio incidento tyrimui reikalingą informaciją, būtina užtikrinti jos integralumą. Vienas iš paprasčiausių būdų – apskaičiuoti perduodamos informacijos (failo) kontrolinę sumą. ***„Windows“*** operacinėse sistemose komandos ***„certutil“*** pagalba galima apskaičiuoti failo ***„md5“***, ***„sha-1“***, ***„sha-256“***, ***„sha-384“*** ar ***„sha-512“*** kontrolines sumas. Skaičiuojant failų kontrolines sumas rekomenduojame naudoti neprastesnį kaip ***„sha-256“*** algoritmą. Pavyzdžiui, ***„certutil.exe -hashfile "D:\memory_dump.raw" sha256“***.

Būtina užtikrinti, kad kibernetinio incidento tyrimui reikalinga informacija būtų **saugoma atskirai** nuo paveiktų sistemų ar įrenginių. Informacijos perdavimą tretiesiems asmenims ar organizacijoms (paslaugų teikėjams) būtina dokumentuoti, pavyzdžiui, pasirašant priėmimo / perdavimo aktą.