eCTHP V2

Hunting End Point

By: Ahmad Abdelnasser Soliman

Index of chapter:

Introduction:

ـ احنا المفروض كل شغلنا الجي مبني على العمليه ال اتعملت سابقا ال هي كان اسمها ال threat intelligence او جالك alertما من ال soc level 1 فتبتدء تشتغل عليه ... يعنى تحت ايدك معلومه ما بتعملها investigation اوانت بنفسك بتروح تدور على ال threat وتبدء تـتعامل معاه خطوة بخطوة ... هل دا معناه انه لو مجلكش alert تحط فبطنك بطيخه صيفي وتطمن !!؟؟ لاء بالعكس ممكن ال attacker يكون اكتشف طريقه تعمل bypass لل defensive methods بتاعتك وعملها تخطي وهو دلوقتي قاعد عندك فالشبكه جوا وبينفذ عليك attack وانت لاتدري .... وزي مكنا قولنا قبل كدا حتى وانت بتعمل investigation متعتمدش على tool واحده لازم تجرب tool تانيه كنظام تأكيدي ... فلازم هنا برضه تأكد على شغلك كذا مرة ومتديش الامان بما ان مجالكش alert !!! بالضبط كدا زي ال شاري fire wall وWaf و Proxy غالي وقاعد مطمن ومستنيهم يبعتلوه ال Alerts .... مش ممكن يكون ال Attacker عملهم تخطي!

وقاعد ف End point من ال عندنا جوا الشبكه وعمال يصيب end point اخرى بال malware وانت لا تدري شيء..... فلازم تدي اهتمام بال End point تماما زى مبتدي اهتمام بال Network .

- انت ك Threat hunter لازم كل يوم تفترض وجود ال Attacker عندك دا جوا عقليتك بحيث تشتغل عال check بتاعك كل يوم وتحاول تثبت عكس كدا عن طريق انك بتعمل check مثلا لل End point وال web server وهكذل من خلال الاكواد الجاهزة ال انت كتبها فال Note عندك حتى من غير مترمي اعتمادك على ال alerts ال بتجيلك من ال Tools زي ال Siem وغيره ... وكمان عشان تقلل فترة ال dwell time ال هي الفترة مابين بالاصابه بأي infection وفترة اكتشافك ليها .... ال هو لوحصلك infection ب malware معين وانت متعرفش وكان حصلك من 4 ايام مثلا وانت اكتشفته انهارده فال 4 ايام دول هما ال dwell time وكلما كان الوقت دا قليل كلما كانت فرصتك ك Threat hunter افضل واحسن لان ال Attacker مش هيكون قدر ينتشر فالشبكه عندك بشكل كبير ويزرع ال malware بتاعه ف أجهزة ال End point ال عندك بشكل أكبر والعكس صحيح .

- احنا المفروض نعرف نعمل Hunting لاي حاجه malicious بدون منحتاج لل Threat intelligence لو انه مهم وهيفيدك فحاجات كتير ولكن عاوزين نعود نفسنا على طرق مختلفه .

- قبل طبعا منعمل Hunting محتاجين نشوف ال End point دي شغاله ازاي وايه ال Process ال شغاله بيها وعلى هذا الاساس هنعرف ال normal منها واي حاجه غير كدا تبقا malicious وهكذا .... وال End point دي زي الاجهزة المتصله بالشبكه زى ال Laptop وال pc وال printer وال server وغيره من الاجهزة المتصله بأطراف ال Network .

- وهتلاقي فالمقابل ال server مينزلوش تحديثات كتير زي ال windows العادي او اي نظام اخر ... فالسيرفرات سهل جدا انك تعملها monitor بالمقارنه بال Desktop machine فهتلاقي معظم المشاكل ال بتجيلك من ال End point بتجيلك من ال Desktop machine على عكس ال servers ال مشاكلها بتكون قليله ومحدودة ... وطبعا دي بتختلف من شركه لاخري لان فيه شركات بتعمل permissions للموظفين ال عندها فحته ال privilege دي بمعني مش كل الموظفين بيكون عندهم نفس الصلاحيات عشان ميعملش حاجه هو مش فاهمها بال Administrator مثلا لو معاه صلاحيه زى كدا ... فالشركات بتدي كل موظف الصلاحيات المتوافقه مع مهامه وممكن كمان تكون على files او folders معينه بحيث تقلل من ال Risk ال ممكن يسببها الموظف دا خصوصا لو كان جديد فالعمل .

- اما فالشركات الكبيرة هتلاقي ان عندهم حاجه اسمها ال Budget بمعني عندهم ميزانيه معينه مخصصه لشراء أجهزة ال Hard ware الخاصه بالحمايه وبيستثمروا في قطع hard ware غاليه جدا على الشركات المتوسطه والصغيرة ال ممكن تستبدل الكلام دا بأنها تعمل install ل service معينه مثلا او تعمل install ل fire wall مش على قد كدا مش professional زى الشركات ال Enterprise .

- احنا هنشوف ال Windows core process وكل process هنشوف مهمتها ايه فالنظام وبعد كدا هنشوف ال normal behavior بتاع ال process بتشتغل ازاي ... ودا عشان ممكن ال attacker ينتحل شخصيه process موجوده عندك عالنظام او يعملها migrate زي ال calc.exe الخاصه بال calculator مثلا ويبتدي يزرع نفسه جوا الجهاز عندك ويسمي نفسه بأسم core process شغاله عندك عالنظام عشان محدش يشك فيه أو يقدر يعمله Detect وينفذ أوامر malicious عندك وانت لاتدري من أين جاءتك .

ودا ال attacker بينفذها في مرحله ال post exploitation ال
هي ما بعد الاختراق عشان ياخد صلاحيات أعلي على جهاز ال victim

Windows Processes:

- عاوزين فالاول نتعرف على كام حاجه عن ال processes زي ...

عاوزين لو لقينا process شغاله على ال End point نشوف اول
حاجه هي parent ولا Child بمعني .. ال parent ال هي
process بيشتغل معاها كذا process تانيه مبتشتغلش لوحدها بيبقى
وراها كذا process شغالين معاها ... اما ال Child دي بتكون
process شغاله لوحدها .

- طب عاوزين نعرف الفرق بين ال process وال service ؟؟؟؟

ال process دي بتكون شغاله على نظام التشغيل أو ال
Application اللي شغال عليه ... زي مثلا اما تفتح fire fox
بيتلاقيه فال task manager مكريت لنفسه process بتنتهي اما
تقفله ... وزي اما بتعمل login فالنظام عندك بتتعمل create ل
process عندك برضه وهكذا دي ال process .

- أما ال service دي بتكون شغاله مع النظام بأستمرار حتى لو انت
وقفت اي service عندك هي هتلاقيها بتعمل restart لنفسها مع
النظام من تاني ودايما شغاله فال back ground عندك ولو عاوز
تعملها ايقاف عادي بس مش هتستفيد حاجه الا فبعض الحالات ... لكن
في ال process الدنيا معاك عادي تقدر تنهي process معينه او
تسيبها شغاله عندك option انك بعد اما تخلص النظام بيعملها
terminate عادي برضه وبرضه عندك فالنظام فيه process معينه
هتلاقي ممنوع تيجي جنبها لانها خاصه بالنظام نفسه وهكذا ....

- ومحتاج اعرف كل process بتشتغل كparent process ولا ك child process لاني محتاج دا ومحتاج اعرف ال normal بتاع ال process المهمه عندي شغال ازاي عشان اعرف اعمل detect لل suspicious ... مثلا لو فتحت fire fox ايه ال parent process ال بتتكون على جهازك وهل تحتيها child process ولا لاء وهكذا وتشوف هل ال process ال لاقيتها دي شغاله normal ولا فيه حاجه مشكوك فيها زي انها بتسحب من ال CPU وال RAM كتير ... ال process ال شغاله دي بتستهلك من موارد الجهاز كتير ولا لاء ولو بتستهلك تعرف انت بتستهلكه فأيه!!

- وكل process شغاله عندك بيبقا ليها path معين بتشتغل فيه .. فال attacker اما بيجي يلعب فال process ال عندك يعملها migration فال post exploitation مثلا هتلاقيه بيغير ال path بتاع ال process ال لعب فيها او غيرها .. فاحنا محتاجين نعرف ال path الاصلي بتاع كل process ال بتشتغل فيه ونحدد اذا كان ال process دي شغاله صح ولا دي malicious .

- كمان محتاج اعرف أسم ال process والحروف بتاعتها وتتأكد من اسمها كويس وانك شايف الحروف كويس ... عشان ال attacker أما بيجي يعمل spoofing ل process ما بيلعب فالحروف بتاعها بحيث انك متلاحظش اي اختلاف ... مثلا زي CALC.exe يلعبلك فيها ل CAIC.exe هو غير حرف لكن انت لازم تلاحظ التفاصيل دي .

- ولازم نشوف كل process ايه هو ال SID بمعني عندنا بعض ال process مبيشغلهاش الا ال Administrator وبعض ال process التانيه لازم ال يشغلها يكون معاه صلاحيات ال System

وفيه process ال يشغلها يكون normal user عادي .. فكل process عندك لازم تكون عارف مين ال المفروض يشغلها ال هو ال security identifier ... عشان وانت بتعمل investigation مثلا هتلاقي user مشغل process معينه وانت عارف ان ال process دي محدش بيشغلها الا ال Administrator فتبدء تشك وتروح تشوف ال user دا مين وتعمل investigation وهكذا ....

- لازم برضه تبص عال process هل هي signed من Microsoft ولا لاء ... وبما اننا بنتكلم عن نظام ال Windows فال process كلها هتبقى signed من Microsoft عشان لو شفت اي حاجه غير كدا هتبقي ال attacker ال مصنعها وعملها creation .

- لو بصيت على كل process هتلاقي ليها name و purpose و ليها path بتشتغل منه وايه هو ال parent process بتاعها و ايه هو ال security ID .... ولكل نظام تشغيل ال process الخاصه بيه

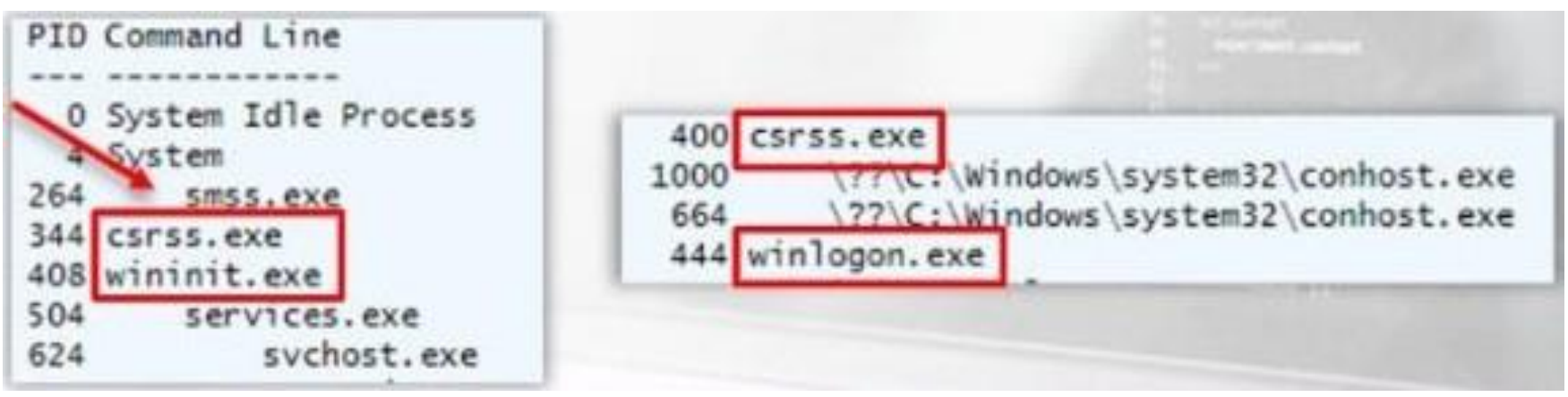
- تعالى نتكلم عن ال process المهمه و أول process عندنا وهي ال SMSS.exe ودي اختصار session manager sub system ودي شغلتها انها بتعمل create لل New sessions عندك ع الجهاز ودي بتشتغل أول مبتشغل الويندوز بتاعك وانت بتعمل power on للجهاز بتاعك .... ال process دي اما بتشتغل بتتقسم لجزءين وهم ال session 0 وال session 1 .

- ال session 0 مسؤله عن تشغيل النظام أو ال operating system الخاص بال windows .

- اما ال session 1 مسؤله عن ال user session بتاعتك اما بتحط ال user name وال password بتتفتحلك session ع الجهاز عندك .

- ال process ال هي SMSS.exe دي parent process يعني بتشغل تحتها process تانيه زي فال session 0 المسؤله عن ال system بتشتغل تحتها process تانيه زي ال csrss.exe وال wininit.exe ..... وهتلاقي فال session 1 المسؤله عن ال user بتلاقي شغال تحتها process تانيه وهي ال csrss.exe وال winlogon.exe ... وبتلاقي ال parent process زي ال SMSS.exe شغاله مرة واحده فقط وبتشوفها مرة واحده فقط .

- هتلاقي ال SMSS.exe أول مبتشتغل بتعمل لنفسها terminate وبعد كدا هتلاقي ال session الخاصه بال Windows operating system بتشتغل واما بتعمل تسجيل دخول بال user هتلاقي ان ال session الخاصه بال user هي ال شغاله بس والباقي معموله terminate .



- تعالى نشوف المسارالتنفيذي بتاع ال process ال هي SMSS.exe بيكون فين ع الجهاز ... هتلاقيه بالشكل دا ....

%System Root%\System32\smss.exe

- فهتلاقيها شغاله فمسار ال root التابع للنظام وليكن ال C partition جوا ال المسار أو ال Folder ال هو System 32 وفيه ال Process بتعتنا ال هي smss.exe .... فلو انت Threat Hunter فتروح تشوف ال process دي شغاله فين وتتأكد انها شغاله فالمسار بتاعها مش فمسار أخر!..... وكمان هتلاقي ال parent بتاع ال process دي هو ال System ذات نفسه ملهاش process تانيه بتشغلها بمعني ان الاب بتاع ال process دي بيكون نظام التشغيل نفسه بمعني ان نظام التشغيل أول مبيشتغل بتشتغل ال process دي معاه .

- هتلاقي ال بيشغلها هو ال System زي مقولنا وهتلاقي ال user name بتاعها هو ال System فلازم انت ك Threat hunter تتأكد ان ال System ال مشغلها مش User عادي !!

- وهتلاقي كمان ليها Base priority رقم 11 بمعني ان ال process دي ليها اسبقيه انها تشتغل قبل اي process تانيه ال priority بتاعتها أكبر من رقم 11 بمعني ان دا رقم الترتيب بتعها فالتشغيل من ضمن process موجوده عال System وكل process ليها رقم معين بتشتغل من خلاله .

- بالنسبه لل session 0 ال هي جزء من ال SMSS.exe زي مقولنا دي هتلاقي ال Time of execution بتاعها ثواني قليله منذ اقلاع ال System .

- تعالى نشوف ال Hunting Tips لل process دي .. بمعني تعالى نشوف ال أحنا ك Threat Hunters هندور عليه فال Process دي بحيث نقدر نقول عليها suspicious او نشك فيها بشكل عام ....

- فال Normal قولنا هتلاقي ال SMSS.exe بتعمل create لل session تانيه تحتها على شكل process ال هما Session 0 وال Session 1 تمام كدا .. دا ال Normal انما لو لقيت ال Sessions تانيه زياده معمولها Create زي مثلا Session 2 و Session 3 وهكذا....

- فممكن تلاقي Session زياده مفتوحه عندك نتيجه ان Attacker مثلا فاتح عندك RDP ال هو Remote Desktop Protocol او واحد بيعمل share لحاجه معينه... طب لو انت متأكد ان محدش فعلا دخل عال System عندك بطريقه Remotely عشان يفتح Session جديده ... تبدء انت تشك فال Session دي وتروح تعمل Deep Investigation بنفسك وتشوف مين ال فاتح ال Session دي .

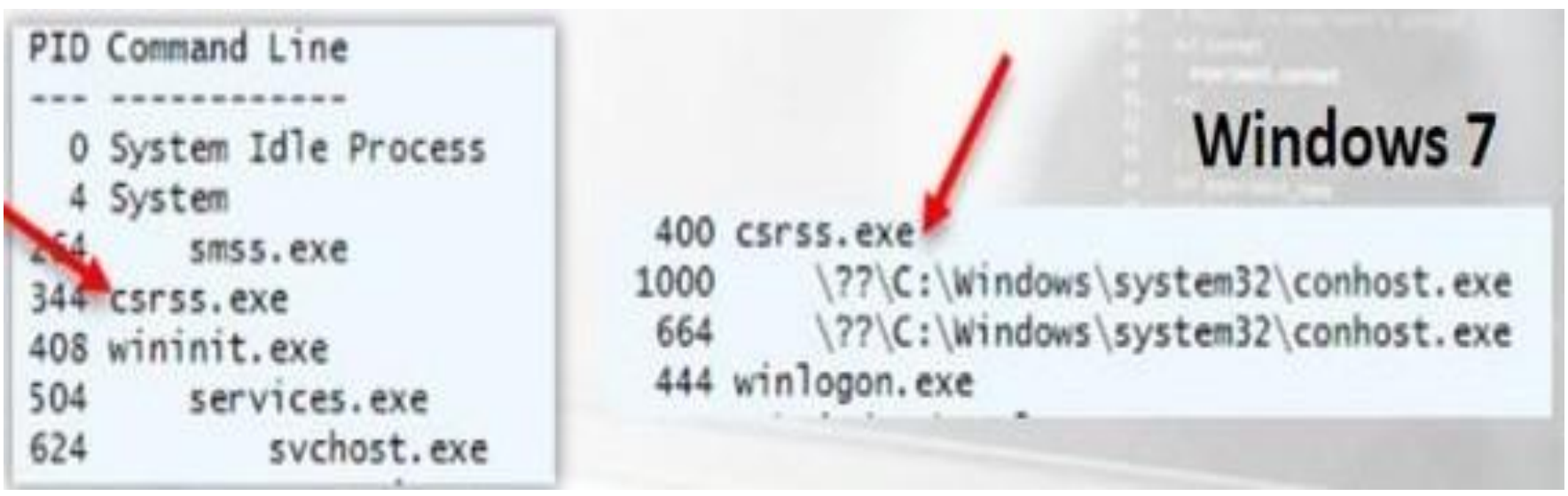
- بمعني اكثر وضوحا .... انت شغلت ال System عندك اشتغلت معاه ال Process ال اسمها Session 0 بتاعت ال Boot ودي بتنتهي مجرد منتا تعمل Login in بأستخدام ال User بتاعك بتبدء Session 1 تشتغل عندك ال هي خاصه بال User تمام كدا .... انت تركز في ان ال SMSS.exe بتلاقيها شغاله مرة واحده عندك عال System متلاقيهاش مكررة لانها بشتغل بس اما بتيجي تشغل جهازك عشان تعمل Create لل Sessions الخاصه بال Boot والخاصه بال User .

- عندنا ال process ال بعد كدا وهي ال CSRSS.exe ودي اختصار لى client/server subsystem process زدي المسؤله انها بتعمل ادارة لل process الموجودة عندك عال System ...بمعني احنا قولنا ان ال SMSS.exe دي مسؤله عن الprocesses الخاصه بال System وانك ك User ت create ال Process الخاصه بيك وهكذا ال system ... انما تيجي لل CSRSS.exe هتلاقيها هي المسؤله عن اداره ال process ال بتنشأ ع النظام بعد الشغل ال قامت بيه ال process ال اسمها ال SMSS.exe.

- وكمان هتلاقي ال Process دي مسؤله انها تعمل create لل drives زي ال C partition وال E partition وال D partition وهي كمان مسؤله انها تعمل create لل Temporary files الموجودة عندك ع النظام وكمان ال Process المسؤله عن ال Shut Down هي ال بتعملها.

- ودي بتشتغل فال session 0 وال session 1 يعني أول مال SMSS .exe بتشتغل دي بتشغل معاها ... ولما ال session 0 بتنتهي ويشتغل بدالها session 1 ال CSRSS.exe بتشتغل معاها.

وال process دي ال هي CSRSS.exe أول مبتعمل create لاي session جديده ال process دي بيتعملها create معاها علطول



- هتلاقي ال Process دي شغاله من المسار دا ...

%system Root%\system32\csrss.exe

- ودي عباره عن child process من ال parent process ال هي SMSS.exe وهتلاقي ال Base priority بتاعتها رقم 13.

وال بيشغل ال process دي هو ال System وهتلاقيها بتشتغل ف ثواني بعد اما SMSS.exe تشتغل بال 2 sessions بتوعها .

- تعالى نشوف ال Hunting Tips لل Process دي ونشوف ازاي نعملها Hunt ....

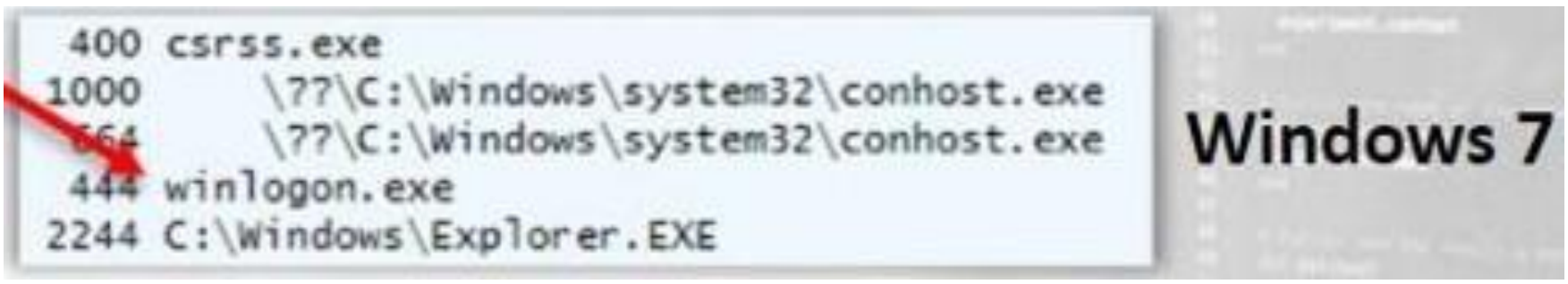
- الشخص ال بيعمل ال malware دايما وهو بيعمل ال Malware هتلاقيه بيتنكر فال process دي ال هي CSRSS.exe فهتلاقيه دايما بيتلاعب بأسم ال process معتمد على عدم تركيزك انت فهتلاقيه بيكتب CSSRS.exe أو CRRSS.exe معتمد على عدم تركيزك وانت بتعمل Investigation فال Processes وأسماءهم وهو حاططلك ف النص malicious process .... فأنت لازم تكون مركز فكل process عينك بتشوفها وتتأكد من أسمها هل هو صحيح ولا لاء .

وكمان هتلاقي ال process دي موجودة مرتين فقط .. مرة فال session 0 والتانيه فال session 1 .

- عندنا ال Process التالته معانا وهي ال Winlogon.exe ودي اختصار ل Windows logon process ودي مسؤله انها تعمل log in او log out لل user اما يجي يدخل لنظام ال windows.

مش انت اما بتيجي تعمل تفتح نسخه ال Windows بتاعتك بتلاقي طلعلك Tab اسمها ال Username and Password .. المسؤول انه يطلعلك ال Tab دي هي ال winlogon.exe .

ـ فأنت بتدخل ال credentials بتاعتك بتقوم ال process بتعتنا ال هي Win logon.exe بتاخد الكلام دا وتبعته ل Process تانيه اسمها LSASS.exe ودي ال process ال بتاخد ال credentials بتاعتك وتروح تعملها Check فال Active Directory لو انت ويندوز سيرفر ... ولو انت ويندوز عادي تروح لملفات ال Local SAM ال متخزن فيهم ال Password وتقارنه وتشوفه صحيح ولا لاء ....وعلى حيث كدا بتبدء تعملك log in أو log out .... وبتشغل process تانيه تحتها اسمها ال Userinit.exe.



ـ وال path الموجودة فيه ال process دي هو ...

%systemRoot%\system32\winlogon.exe

ـ ملحوظه كدا ... ال folder ال اسمه system 32 دا مهم جدا لان فيه أهم process بتشغل ال windows فخد بالك اوعي تلعب فحاجه فالفولدر دا.

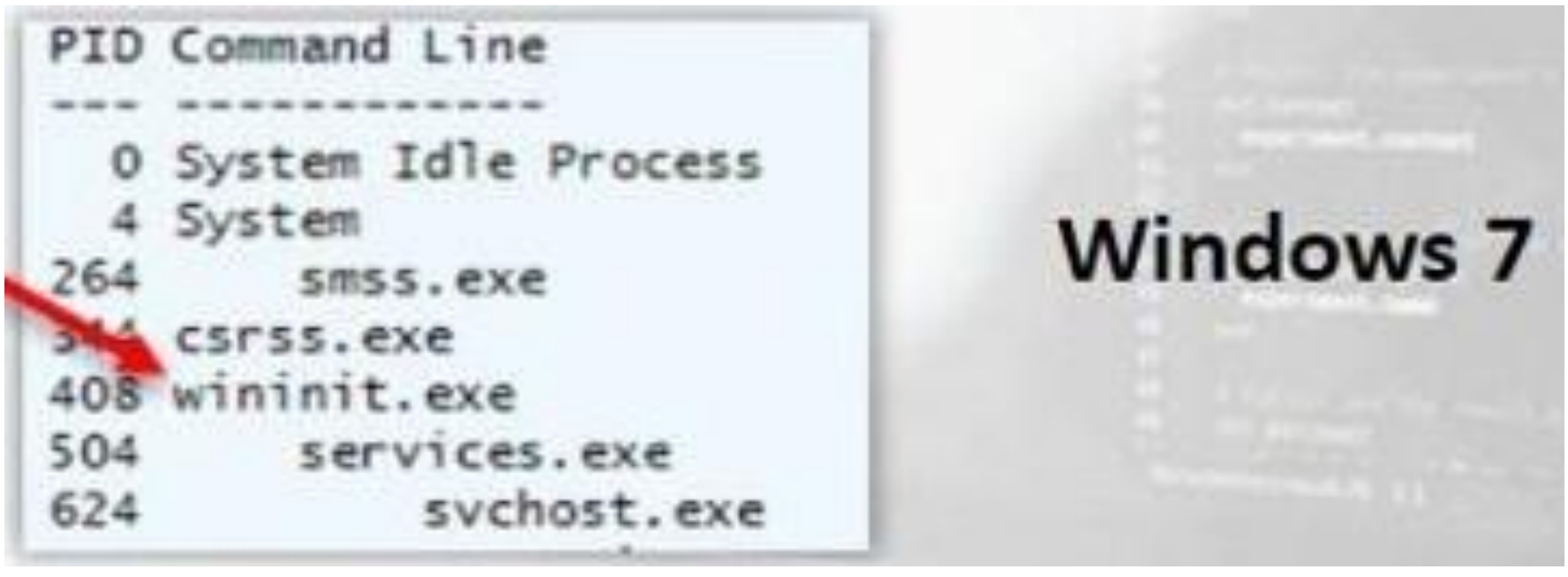
ـ وكمان هتلاقي ال winlogon.exe دي child process ال بيشغلها هو ال SMSS.exe وال SMSS.exe ال بيشغلها هو ال System.

والمسؤول انه يشغل ال process دي هو ال System وال priority بتاعتها هي 13 وبتشتغل علطول بعد session1 بتاعت ال boot .

ـ تعالى نشوف ال Hunting Tips لل process دي ال اسمها Winlogon.exe ... دي مش هنعرف نشوفها زي ال processes ال فاتت لازم نبص على ال registry Value بتاعت ال process دي .... ومكتبه ال registry دي مكتبه رقميه بيتسجل عليها كل حاجه بتحصل عال System عندك ... فالمفروض ان ال process ال winlogon.exe بتاخد جزء من المكتبه دي ...

ـ فهتلاقي ال attacker بيروح لل registry file الخاصه بال process ال اسمها Winlogon.exe ويبدء يتلاعب بالحتوي الموجود جواها.

ـ عندنا ال process الرابعه معانا هنا هي ال Wininit.exe ودي اختصار لي windows initialization process ودي مسؤوله عن تشغيل process أخرى زي ال Service وال lsass.exe وال lsm.exe .... وهتلاقيها بتشتغل مع ال 0 session من ال process ال اسمها SMSS.exe ولازم ال process ال Wininit.exe تشتغل عشان تنادي على باقي ال process المتخصصه فأنها تقوم بعمليه ال user logon وغيرها من ال process اللازمه لل windows .



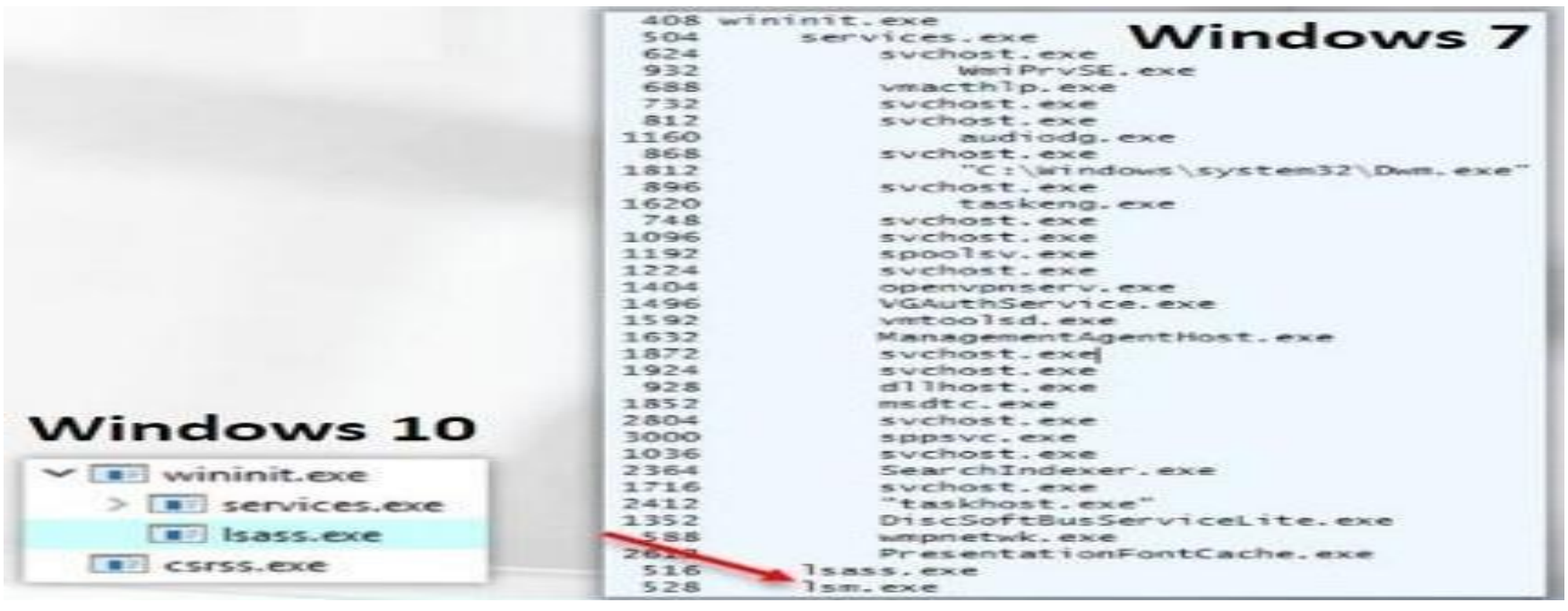
- وهتلاقي ال process دي ال بيشغلها هو ال system من المسار %systemRoot%\system32\wininit.exe

- ودي برضه عبارة عن child process من ال SMSS.exe وال priority بتاعتها 13 وبتشتغل فوقت قليل من عمليه ال Boot الخاصه بال System

- ال Hunting Tips بتاعتها بتكون ان ال Wininit.exe بتكون ليها 1 instance فقط .... بمعني هتلاقي ال process دي شغاله مرة واحده بنفس الاسم مينفعش تلاقيها هي هي متكررة فنفس الوقت .

- ال process السادسه معانا هي ال LSM.exe ودي اختصار ل Local session manager ودي بتشتغل مع ال SMSS.exe عشان تعمل create او destroy ل service معينه لاي user session معينه ... مش احنا قولنا قبل كدا ان ال SMSS.exe دي بتشتغل عشان تعمل manage لل processes الخاصه بال System بس مش هتقدر تقوم بعمليه ادارة كل ال Processes الخاصه بال system فعشان كدا بتشغل ال LSM.exe عشان تساعدها فعمليه اداره ال Sessions الخاصه بالنظام .

- وكمان هتلاقي ان ال process ال اسمها LSM.exe مسؤوله انها تعمل logon و logoff لل system وبتعمل start لل Shell وبتعمله End .



- هتلاقي ال parent process بتاعتها هي ال Wininit.exe وهتلاقيها موجودة فالمسار دا ....

%systemRoot%\system32\LSM.exe

وهتلاقي ال priority بتاعتها 8 والمسؤول عن تشغيلها ال System وال بيشغلها ال Wininit.exe بعد اقلاع ال System بثواني بسيطه

- تعالي نشوف ال Hunting Tips بتاعت ال Process دي ماشيه ازاي ... هتلاقي فال Windows 7 ان ال process دي ليها 1 instance فقط .... انما ف Windows 8,10 مش هتلاقيها بنفي الاسم وهتلاقي اسمها اتغير لاسم Service تانيه ال هي DLL وهتلاقي اسمها LSM.DLL وبرضه هتلاقي ال Service دي شغاله 1 instance .... فلو لقيت حاجه متغيرة عن كدا وانت بتعمل Hunt أعرف انها suspicious وتعملها Detect علطول .

- عندنا واحده من اهم ال processes ال شغاله أالا وهي ال Services.exe وادي اختصار ل Service control Manager

ودي مسؤوله انها تعمل loading لكل ال Services الخاصه بالنظام عندك سواء كانت الخاصه بال drives او system نفسه وبتشغل كل ال Services دي وتحطها جوا ال Memory بتاعتها .

وهتلاقيها موجوده فالمسار دا وهو .....

HKLM \ SYSTEM \ CURRENT CONTROL SET \ SERVICES.

- وكمان هتلاقي ال services.exe هي ال parent process ل process زي ال svchost.exe وال dllhost.exe وال task host.exe وال spoolsv.exe وعندك processes أخرى كتير مش هنذكرها هنا ال بيشغلها هي ال services.exe.

- وهتلاقيها ال parent process بتاعتها هي ال wininit.exe وال بيشغلها هو ال system وال priority بتاعتها هي رقم 9 وبتشتغل بعد ثواني من اقلاع النظام عندك .... وهتلاقيها موجوده فهذا المسار....

%systemRoot%\system32\services.exe

- ال Hunting Tips لل processes دي هتلاقي انها شغاله ب 1instance فقط ..وكمان هتلاقيها protected ال process دي يعني محدش يقدر يلعب فيها الا ال System فقط.... فأنت لو لقيت حاجه شغاله غير كدا اعرف انه suspicious واعملها detect علطول .

- عندنا ال process ال بعدها وهي LSASS.exe وهي اختصار ل local security Authority subsystem ودي مسؤوله انها تاخد ال Authentication بتاع الuser من ال Active Directory لل Windows Server وال SAM files للويندوز العادي وتحوله لحاجه اسمها 'Tokens ال بتستخدمهم علطول وانت بتعمل عمليه ال login الخاصه بال user .

- وكمان جوا ال security event log ال بيعمل Write جواه ويكتب مين عمل login ومين فشل ومين نجح هي ال process ال LSASS.exe .

- هتلاقي ال parent process ليها هي ال Wininit.exe ودا المسار الموجوده فيه ...

%systemRoot%\system32\LSASS.exe

والمسؤول انه يشغلها هو ال System كالعاده وال priority بتاعتها هي رقم 9 وبتشتغل بعد ثواني من عمليه اقلاع النظام .

- خد بالك من نقطه اننا اما نيجي نعمل Hunt بنبص على ال keys دي ال هما المسار الموجود فيه ال process ومين ال مشغلها ومتحكم فيها وال priority number الخاصه بيها ... وهكذا .

- ال Hunting Tips لل process دي هي ان ليها 1 instance فقط.

هتلاقي ال attackers بيستغلو ال process دي كتير فال attacks بتاعتهم لانهم بيعوزوا يقروا ملفات ال passwords وال Hashes ال متخزنه فجهاز ال victim فبيروح ال Attacker عامل create ل process شبيهه لل process الاصليه .... وليكن مثلا ال LASS.exe وبيعمل ال attack بتاعه عادي ويثبت عند ال victim ال malware على شكل ال process دي ويبدء من خلالها يسرق ال passwords ودا حصل بالفعل من خلال هجوم Stuxnet Malware .

- ال process ال بعدها وهي ال Svchost.exe ودي اختصار لي Generic Service Host Process ... وانت عندك كل host او جهاز عليه بعض ال Services شغاله عليه وعندك بعض ال Processes لازم تشتغل مع بعضها عشان تطلعلك النتيجه ال انت عاوزها من ال process دي ... فلو process عاوزه تتواصل مع process اخرى المسؤول عن الكلام دا هي ال Svchost.exe.

- هتلاقي ال parent process بتاعتها هي ال services.exe وهتلاقي ال بيشغلها هو ال System او ال user او ممكن تشتغل ك service فال network عندك ... ودي تقريبا أول process معانا يقدر يشغلها user عادي غير ال System فخد بالك من الحته دي برضه ..... وال priority بتاعتها رقم 8 وهتلاقي المسار الموجوده فيه هو.... %systemRoot%\system32\Svchost.exe

كمان هتلاقي ال Time of execution بتاعها بيختلف شويه عن ال processes ال فاتت هتلاقيه various بيختلف من ال System لل User وطبعا هتلاقي فال System بيشتغل أسرع من ال User العادي.

- تعالى نشوف ال Hunting Tips بتاعت ال process دي ....

ال attacker ممكن يستخدم ال process دي عشان يعمل launch لل malware ال مثبته عندك عالجهاز ويستغل ال service ال هي Svchost.exe عشان ينفذ ال Attack بتاعه .

وكمان هتلاقي ال Attacker بياخد ال malicious process ال عاملها دي ويوزعها على directories كتير وبيغير اسمها بحيث يخفيها ان اي حد ممكن يعملها Detect ... وممكن ينسب ال Service دي ل parent process غير ال Services.exe بحيث برضه متعرفش تعملها Detect .

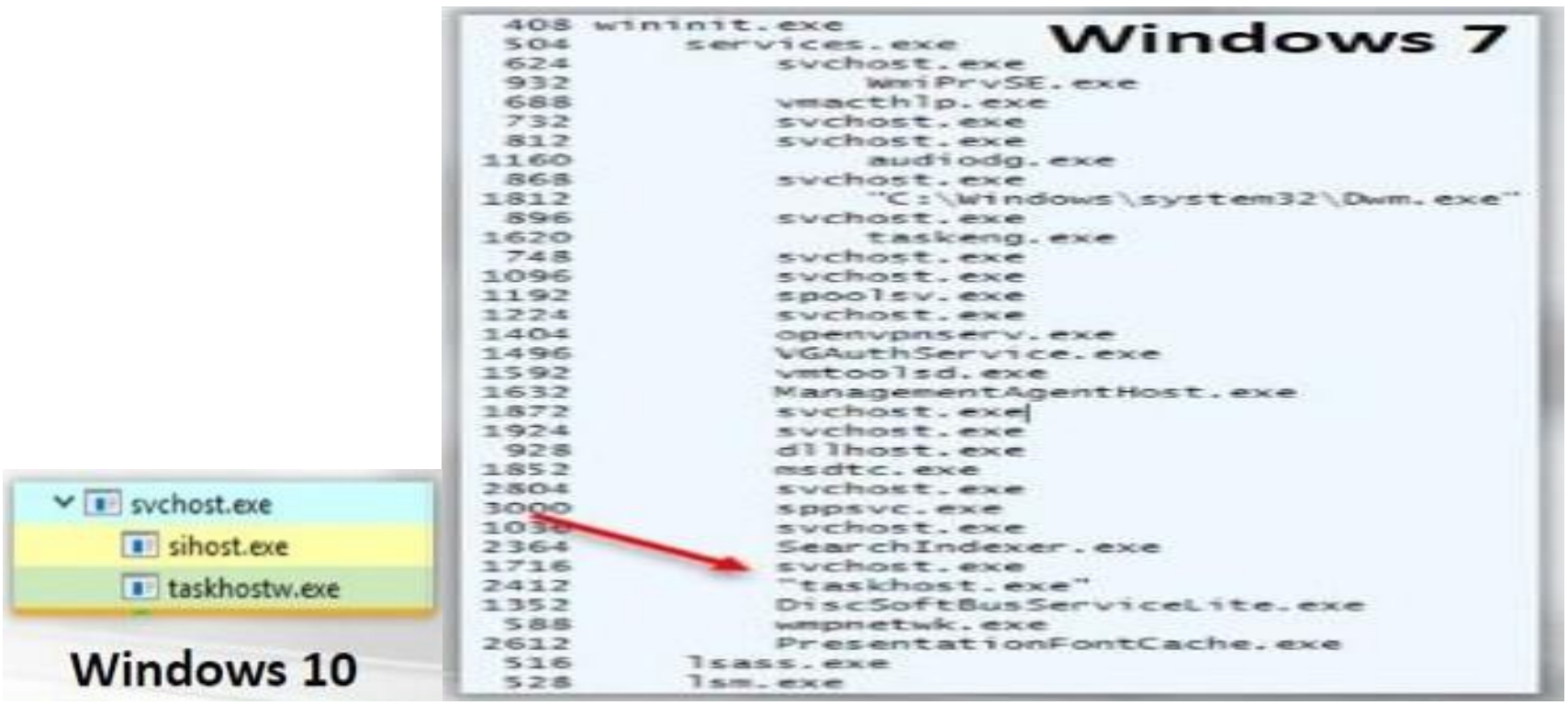
- فأنت وانت بتعمل Hunt تبص على ال path بتاع ال process وتبص على ال parent process بتاعتها ومين ال مشغلها وتبص كمان على ال priority بتاعتها واستهلاك ال process من ال CPU تمام ولا على غير المعتاد والوقت ال اشتغلت فيه لما كان ال system مشغلها قليل ولا خدت وقت طويل ولما ال user شغلها وهكذا ... تقعد تملا على ال processes المهمه عندك وتشوفها وتعملها

investigation وتشوف ال normal بتاعها ماشي تمام ولا لاء عشان تعرف ت Hunt ال malicious منها .

- تعالى نشوف ال process ال بعدها وهي ال taskhost.exe ودي هتلاقيها اختصار لى Generic host process ... انت عندك ال processes اما بتشتغل بيكون ليها ملفات تنفيذيه .exe بتشتغل معاها وبعض ال processes الاخري بيكون ليها ملفات DLLs ال هي بتيجي من مكتبه ال Windows نفسها .... فلو انت بتشغل process من الموجودة في مكتبه ال windows نفسه هتلاقي المسؤول عنها هي ال Taskhost.exe .

- وهتلاقي اسم ال process دي بيختلف من نوع windows لاخر مثلا فال windows 7 هتلاقي اسمها زي مهو Taskhost.exe اما في ال Windows 8 هتلاقي اسمها Taskhostex.exe اما فال Windows 10 هتلاقي اسمها Taskhostw.exe.

فال process دي وظيفتها انها تشغل ال processes الاخرى ال ملفاتها من النوع DLLs مش من النوع exe .

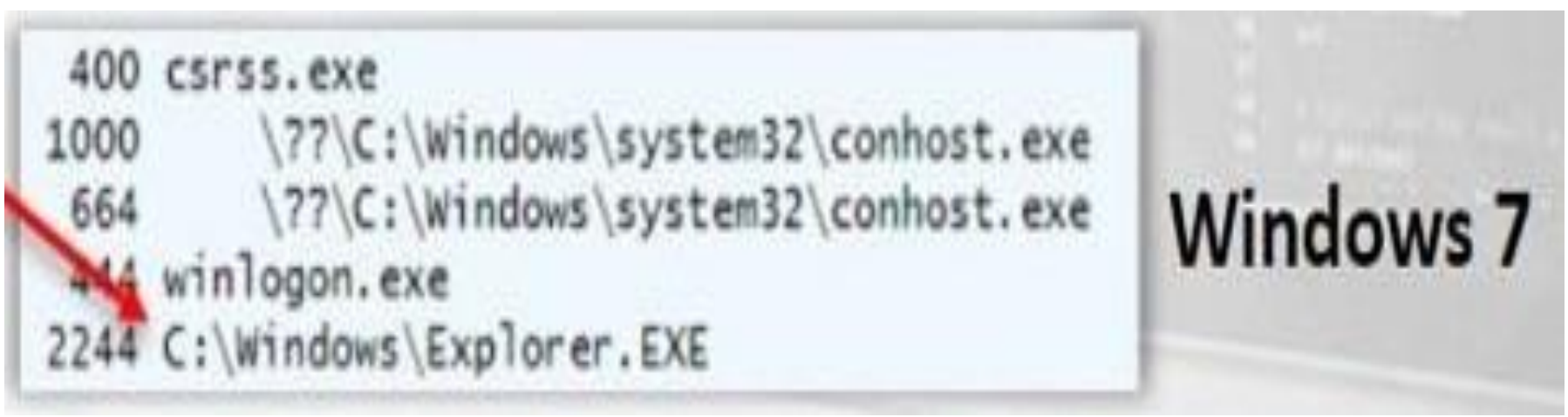


- وهتلاقي ال parent process بتاعتها هي ال services.exe ال بتشغلها يعنى .... واسم ال process دي هتلاقيه various بيختلف من شخص لاخر يعني ممكن ال System هو ال يشغلها و ممكن ال User هو ال يشغلها عادي بتختلف من شخص لاخر ... وال priority بتاعتها رقم 8 وهتلاقي الوقت ال بتشتغل فيه various برضه من ال system لل User .... وهتلاقيها موجوده فالمسار دا ....

%systemRoot%\system32\Taskhost.exe

- وبالنسبه لل Hunting Tips هتلاقي ملهاش حاجه Specific تقدر تعملها detect بيها .... الا الحاجات ال ذكرناها فوق وال تقدر من خلالها تعمل detect لل process دي لو كانت malicious .

- تعالى نشوف ال process ال بعدها وهي الخيرة معانا ... وهي ال explorer.exe ودي اختصار لل Windows Explorer ودي مسؤوله عن ال User Desktop واي حاجه بتظهر عند ال User على ال Desktop زي الايقونات ال بتظهر عندك عال Desktop والقوايم ال بتظهر عندك وهكذا ... والساعه والتاريخ والنوافذ ال بتظهر عال Desktop كل دا المسؤول عنه هي ال explorer.exe ... ودايما هتلاقيها شغاله عندك فال windows اما بتيجي تشغله ... ولو انت مشغل برامج كتير عال windows هتلاقي ان ال process دي شغاله مرة واحده فقط لكل البرامج مش لكل برنامج process شغاله ليه .



- هتلاقي المسار الموجوده فيه %SystemRoot%\explorer.exe مش زي ال process ال فاتت خد بالك فلازم تتاكد انها شغاله من المسار دا ... وال parent process المسؤول عن تشغيلها هي ال userinit.exe .... وال بيشغلها بيكون على حسب ال user ال عامل login عالجهاز حاليا برضه خد بالك فيه اختلاف عن ال processes ال فاتت .... وال priority بتاعتها رقم 8 والوقت ال بتشتغل فيه بيبقى various بيختلف من user لاخر .

- ال Hunting Tips بتاعتها هتلاقي ان ال attacker دايما فال attack بتاعه وهو بيستخدم ال malware هتلاقيه بي target ال process دي دايما ... فممكن يعمل inject لاي حاجه malicious زي ال malware جوا ال process دي بحيث كل مال process دي تشتغل ال malware يشتغل معاها عادي .... وممكن يخلى ال process دي تشتغل بأسم أخر من folder مختلف وتنفذ ال attack بتاعه عادي بحيث يبقا صعب عليك تعملها detect .

وممكن يستغل port عندك عالجهاز يستخدمه فأنه يعمل listen عال process دي يشوفها شغاله وبتنفذ فعلا ال malware ال زرعه ال attacker جواها ولا لاء ... ودا هنشوفه بشكل عملي فال modules الجايه باءذن الله .

- ضيف عال 10 processes ال قولناهم فوق وانت بتعمل hunt بص برضه عال out bound IPS بمعني بص عال processes الجديده ال نشأت او اتعملت مع Ip معين على جهازك بص عال processes دي وشوف استهلاكها من resources بتاعت جهازك ايه نظامها وشوف ال normal بتاعها ماشي ازاي عشان لو لقيت حاجه مختلفه عن كدا اعرف انه suspicious ودور انت بنفسك وزود البحث بتاعك عال processes ال من النوع دا وضيفها لل notes

بتاعتك على جنب كدا .... وشوف كمان ال digital signature بتاع ال processes ال core عند فنظام ال windows هل هي من شركه Microsoft ولا لاء وهتلاقي جنب كل process الشركه ال مصنعاها وشوف هل الشركات ال مصنعه ال process دي موثوقه ولا مشبوهه.

- برضه بص عال process المعروفه زي ال CMD وال Power shell وال Wscript كل دول هتلاقيهم exe. ولازم انت تكون مشغلهم وبتنفذ من خلالهم اكواد معينه ... فلو مثلا روحت لل task manager وروحت لل process لقيت الحاجات دي شغاله كدا وانت مستخدمتهاش اعرف ان ال attacker بينفذ اكواد عن بعد باستخدام ال processes دي فتروح تعملها kill بعد اما تتأكد طبعا وهكذا تقعد تعمل investigation بنفسك لحد متتأكد ان كل حاجه normal.

- وفالاخر خالص بتحتاج انك تعمل memory analysis عشان تتأكد ان مفيش حاجه malicious مزروعه وبتتنفذ فالخفاء اما تيجي تعمل start للجهاز بتاعك وانت مش واخد بالك ...ودا برضه هنشوفه بالتفصيل والشرح العملي فال modules الجايه.

End Point Baseline:

- ال Base line كنا اتكلمنا عليه قبل كدا فال Hunting web shell عشان نطلع الحاجات ال anomalies فال System process وال drives وال File structures ... فكان ال base line بيخلينا نعرف الطبيعي بتاع ال Processes مثلا ماشي ازاي عشان لو شفنا غير كدا نعرف انه مشبوه ونعمله Detect .

- فاحنا بنعمل عمليه مقارنه عشان نعرف ال configurations وال current setting بتاعت ال Machine بتعتنا ايه حالتها قبل اي حاجه .... بنحتفظ بنسخه منها عندنا ونرجع نقارنها بالنسخه الحاليه ال شاكين انها Suspicious ونشوف الاختلاف فين ونطلعه وهو دا بيبقا الحاجه ال Suspicious .... فاحنا بناخد لقطه لل End point بتاعتي ال بيحصل عليه configuration اثناء الشغل وباخد اللقطه دي بعد اما اعمل ال installation لل End point ال عندي ودا بالنسبالي احسن وضع ....

- احنا بناخد اللقطه دي لل End point او بنعمل Create لل base line بتعنا بعد اما ال Developer او ال develop team خلص ال updates بتاعته .... وبتقوم واخد لقطه لل System دلوقتي وبعدين تقارنها بالوضع الاسبق (الاصلي) ال خدناه فالاول .... فال Base line بتاعتي لو خليته يطلعلي ال folders ال اتعملها Create او ال اتعملها Change فأنت كدا ك threat hunter هتوفر على نفسك وقت كتير !! لانك مش هتعمل investigation فجميع ال Folders او ال Files .... لاء انت هيطلعلك فقط ال اتعمله change او create فأنت تروح تشوفهم وتعملهم Deep investigation وتبقى وفرت على نفسك انك ت Investigate ال Files بتاعت ال system كله .

- خد بالك من ان الشركه ال بتعملها Hunting ممكن تكون عملت بعض ال updates بدون علمك بيها فنتج عنها create لبعض ال files فال folders ال بتعملها investigation فأنت مش تبلغ الشركه علطول انها suspicious الا اما تتأكد من الشركه نفسها ال شغال معاها انها فعلا متعرفش عن ال files ال متضافه عندها فال End point دي حاجه ساعتها بس تقدر تقول عليها Suspicious.

- عندنا بعض ال Tools الاخري ال بتساعدنا انها تعملنا Detection وبتعملك monitoringلاي تغيرات فال baselineعندنا زي مشرحناه فوق .... زي Solar Wind و Trip Wire و Alien Vault وLog Rhythm و Secure trust .

- لو احنا ك Threat Hunters اكتشفنا ان في file اتعمله create او changeالموضوع هيبقا صعب انك تدخل بايدك manual وتعمل Detect للكلام دا وخصوصا فال Large enterprise وافرض انك لقيت مثلا 1000 file اتعلمهم create بشكل مستجد انت هتعملهم كلهم investigation كدا يبقا احنا بنضيع وقت!! الكلام دا يمشي فال small enterprise .

- احنا عندنا Appliances زي Tools كدا مصمه للكلام دا وعندها database بال malicious content file نديها الكلام دا وهي هتقوم بدورها انها تعمل ال Base line وتقارن ال Files ال هنديهلها بال Files ال malicious ال عندها وبدورها هي هتقولنا اذا كان دا malicious ولا Clean ... وال features ال زي دي الشركات المصنعه لل tools بتضيفها لل tools بتعتها دي زي Solar Wind كدا لو هتشتري منهم Network monitoring devices مثلا للمؤسسه بتاعتك هتلاقيها هي نفسها متبرمجه ع الكلام دا وبتقوم بال Baseline دا من تلقاء نفسها طبقا لل Database بتاعتها وبتطلعلك النتايج النهاءيه .

- عندنا بعض ال Tools ال ممكن احنا نستخدمها عشان نعمل Create لل Baseline بتعنا ال عاوزين نعمله دمج بعد كدا فال end point ال عندنا او فال tools ال بتعملنا monitorلل end pointال عندنا ودا هنشوفه مع بعض فالجي ....

- عندنا اول اداه من Microsoft وهي ال SCCM ودي اختصار ل System Center Configuration manager ... الاداه دي لازملها server environmentعشان تشتغل معاك ... دي بتعمل configuration لكل الاجهزة مره واحده بدون اختلاف بتطبق نفس ال configuration ع الاجهزة كلها على كل ال Domains يعني الموجودين فال Base Line بتاعتك ....

- وال Configuration ال اتعملت عال devices الموجوده فال End Point عندي هاخد منها نسخه احتفظ بيها وارجع فالمستقبل اقارنها بالنسخه الحاليه عندي عالاجهزة واشوف فين التغييرات والفروقات بين الاتنين .... والاداه دي هتلاقيها فال Enterprises الكبيره وال معتمده على نظام ال Windows فعملها .

- الاداه التانيه عندنا لو الشركه بتاعتي معندهاش ال Budget او الميزانيه انها تصرف وتجبلنا ال SCCM .... فهنرجع لل Power shell من تاني فالحاله دي ... وال power shell بيقدر يعمل الحاجات الشبيهه لل SCCM عن طريق حاجه اسمها ال Desired state configuration ودي خاصيه جوا ال Power Shell بتقدر من خلالها تعمل configuration واحده وتبعتها لكل ال End point ال عندك وتتطبق عليهم كلهم .... وال configuration دي تاخدها بعد كدا انها ال Base line لكل الاجهزة ال عندك فال Network بتاعتك ...

- ال tool دي بتسمحلك انك تطبق Configuration واحده على كل الاجهزة وبتسمحلك انك تحتفظ بنسخه من ال Configuration عندك بحيث بعد كدا ترجع تراجع عليها من خلالها وتقارنها بال Configuration الحاليه وتشوف فين التغيير ال حصل.....

- وبكدا بتسمحلك انك تطبق ال Base line عن طريق Scripts فال power shell عندك .... لو انت مهتم بال Automation عندك ادوات زي ال puppet او ال Ansible او ال Chef وغيرها كتير دول بيستخدمهم ال Server Admin عشان يعمل بيهم configuration جديده تطبق عال Users الموجودين عال Server أو يشيل Configuration معينه كان مطبقها قبل كدا .

- الاداه التالته عندنا وهي ال Microsoft Security Compliance Manager ودي اختصارها SCM ودي بتساعدني ان اعمل Deploy لل Policies وال Configuration طبقا ل rules او معايير من وجهه نظر Microsoft شايفه ان دي افضل ودا ال انت ممكن تعمله بنفسك من خلال ال Configuration ال Manual ال ممكن تعملها بأيدك ... فدي ميزة عند الاداه دي عن ال tool ال فاتت انك عندك معايير شركه Microsoft بتوجهك ليها من خلال ال tool دي ... وال Tool دي معتش Microsoft بتنزلها مع ال windows وكمان وقفت تحديثها من فتره بس انت لو عاوز تنزلها manual بنفسك دا متاح عادي وتستخدمها .

- عاوزين نحط احنا Base line لل Services او ال Processes ودا هنعمله من خلال ال power shell اننا هناخد لقطه من ال processes ال شغاله ع االجهاز حاليا او بعد ال updates ال هعملها عال End Points وبعد كدا فالمستقبل اشوف ال processes الجديده ال اتضافت أو اتعملها تشغيل عندي عالجهاز ... وكل دا هنعمله بواسطه Scripts جاهزه هنستخدمها ك Base line عندنا بواسطه ال Power shell ... والكلام دا كله ممكن تستخدمه بعد كدا انك تعمل Hunting لل Malware المتواجد عندك ف End point معينه او تعمل بيه Check لل End point ال عندك عشان تتأكد هل فيه Malware أصاب الاجهزة دي ولا لاء .

- تعالى نعرف مع بعض ازاي ممكن نعمل Base line ل Service معينه عندنا .... زي ال Command دا بالضبط .

```
Get-Service * | Where {$_.status -eq "Running"} | Export-Clixml Baseline-Services.xml
```

- عندنا cmdlet اسمها Get-Service يعني command بتكتبه فال CMDلل Windows عشان يجبلك ال Service ال شغاله حاليا .... وبعد كدا بتقوله * بمعني انا عاوز كل ال services ال شغاله عندي عالجهاز ... بعد كدا علامه ال pipe يعني عاوز تدخل ال commandدا على filter اخر ... وبعد كدا Where يعني بتقوله عاوز اكتب شرط بمعني بتقوله (عندما) وبعد كدا بتديله ال condition بتاعك ال هو عاوز ال Services ال حالتها running .... وبعد كدا علامه ال pipe مرة اخري بمعني كل ال فات دا اعملي ليه filter ودخله عالكلام الجي .. بعد كدا بيقولك اعمله Export يعني تصدير او حفظ لملف XML وسميه Baseline-services.xml .

فالمثال ال فات شوفنا مع بعض ازاي تعمل Base line للservices ال عال End point ما عندي فالشبكه عن طريق ال power shell script .

- فلو حبيت اي وقت ك Threat Hunter اعمل compare لل Baseline ال عندنا ... عندنا command اخر بنكتبه جوا ال PowerShell اسمه Compare-object ودا بنكتبه اما نكون عاوزين نقارن ال Base lines ببعضها .

```
Compare-Object (Import-Clixml Baseline-Services.xml)(Get-Service * | Where {$_.status -eq "Running"}) -Property DisplayName | Where-Object {$_.sideindicator -eq "<="}
```

- ال Commandدا معناه انك عاوز تقارن ال Two Base lines ببعض ... فبتقوله ال Compare-object ال Commandبتاعك ... وبعد كدا بتقوله import يعني تجيب الملف ال Xml ال هو ال Base line الاصلي بتعنا الكنا خدناه فالاول ... وبعد كدا تديله اسم الملف بتعنا ال baseline الاصلي ... وبتقوله بعد كدا عاوز اجيب ال Service ال حالتها Running .... وبعد كدا بتقوله طلعلي ال Display names بتاعتهم ثم طلعلي الاختلافات ال بين ال Files ال هي العلامات دي .... (<=) ال هي ال Side indicators ال عندك .

- طب تعالي نعمل نفس الكلام بس مع ال processes وليس ال Services .... نفس الكلام بالضبط ولكن هنغير ال Cmdlet ال هو ال Command فقط ..... هنحط Get-process .

```
Get-Process | Export-Clixml Baseline-Processes.xml
```

- اهوه نفس الكلام بتقوله هاتلي ال processes ال شغاله وحطهالي في ملف Xmlوسميه بالاسم الموجود دا وهكذا .....

- ونفس الكلام اما تيجي تعمل Compareلل processes ال عندك

```
Compare-Object (Import-Clixml Baseline-Processes.xml)(Get-Process) -Property Name | Where-Object {$_.sideindicator -eq "<="}
```

- اهوه نفس الكلام ال فات فال Services مع الاختلاف اننا شغالين عال processes هنا فال Command دا .... هتلاقيه بيقوله هاتلي الملف ال Baseline لل processes ال عندي وهاتلي الملف الحالي ال Baseline واعملي بينهم compare وطلعلي الاختلاف مبينهم .

- زي مشوفنا مع بعض اننا نقدر نعمل Baseline لل services وال Processes ال عندنا ... احنا كمان نقدر نعمل Baseline لل users ال عندنا ....

- يعنى وانا ب create ال Users لل system بتاعي الجديد ال لسه عمله installation أخدت نسخه او لقطه أو base line منه بال users ال عملتلهم create عال system عندي عشان قدام فالمستقبل ابقا اخد baseline تاني واقارنه بالقديم واعرف هل فيه users جداد تم اضافتهم عندي عالنظام من خلال عمليه اختراق حصلت وانا نايم فالعسل ومعنديش بيها علم .... فال Baselines ال بعملها بتساعدني فالكلام دا .

- وكمان ممكن أخد Baselineلل operating system كله وكمان اقدر أخد Baseline لل System Users ال عندي وكله عن طريق ال Power shell tool بال Scripts دي ودي بتبقى مجهزة مش محتاجه حفظ موجوده فكل مكان وتقدر تاخدها copy و paste عندك فال notes الخاصه بيك ك Threat Hunter اما تيجي تعمل عمليه ال investigation لل End points ال عندك ف Network المؤسسه ال فيها تبقا تستخدمها.

```
Get-WmiObject Win32_UserAccount | Export-Clixml Baseline-UserAccounts.xml

Get-WmiObject Win32_OperatingSystem | Export-Clixml Baseline-OS.xml

Get-WmiObject Win32_SystemUsers | Export-Clixml Baseline-SystemUsers.xml
```

-وكمان انت ك Threat Hunter وانت بتعمل Investigation فال End points عندك تاخد معاك Baseline لل Accounts الموجوده عال System وال Users وال Services وال Processes ال عندك عال System .... وكمان ال Local administrator عال System عندك ... وال Folder contents وال Folder permissions وال Tasks Folder وال Network folders containing internal installation وهكذا اي حاجه انت شايفها مهمه ولازم تعملها Base line ك Threat Hunter لازم تاخدها فسكتك .... وال Scripts الخاصه بال Commands دي موجوده على Google تقدر تبحث عنها براحتك ..... تقوم كاتب ف Google هكذا فالبحث تكتب Cmdlet لكذا وليكن لل services هتلاقي ال command طلعلك تاخده Copy و paste عندك وتبقى منظم فشغلك عشان كل متكون منظم ومرتب كل متوفر وقت ومجهود على نفسك .

- وبكدا نكون انهينا ال Module دا بفضل الله وبكدا نكون غطينا النقط دي ....

- اننا عرفنا اغلب ال Windows core processes وعرفنا ازاي نقدر نحدد اذا كان ال processes دي عاديه النظام هو ال مشغلها أو نقدر نقول عليها انها شغاله عن طريق malware اصاب الجهاز عندنا.

- عرفنا برضه اهميه اننا نعمل Baseline لcreate عندنا عال Endpoints بواسطه ال tools المدفوعه من Microsoft زي SCCM والمجانيه ال جايه فنظام Windows زي ال Power Shell عشان نعرف نعمل Hunt لاي Malware يكون عندنا فالنظام بشكل سليم ومنظم.

---مش محتاج افكرك بالدعاء بالنصر لاخوتنا المستضعفين فكل مكان.