استاکس*نت با استفاده از روش*های مختلفی تکثیر می*شود. این بدافزار می*تواند خود را با استفاده از درایوهای قابل انتقال منتقل نموده، و یا با سوء استفاده از دو آسیب*پذیری در سطح شبکه خود را کپی نماید. علاوه بر این، استاکس*نت می*تواند با منتشر شود. با استفاده از این روش، با هر بار اجرای پروژه، استاکس*نت اجرا Step7 استفاده از کپی کردن خود در پروژه*های .می*شود. زیربخش*های زیر این سه روش تکثیر را توضیح می*دهد

روش*های تکثیر در شبکه ·

Network"\ اکسپورت 22 مسئولیت اصلی روش*های انتشار استاکس*نت در شبکه را دارا می*باشد. این اکسپورت یک کلاس می*سازد که شامل 5 زیر کلاس می*باشد. هر زیرکلاس مسؤول یکی از روش*های آلوده*سازی یک میزبان راه دور "\Action .می*باشد

:عملکرد 5 زیرکلاس مذکور از قرار زیر است

ارتباط و به*روز*رسانی*های همتا به همتا ·

با استفاده از گذرواژه کارگزار پایگاه داده*های کد شده WinCC آلوده*سازی ماشین*های ·

انتقال با استفاده از به*اشتراک*گذاری*های شبکه ·

(Print Spooler) MS10-061 انتقال با استفاده از آسیب*پذیری افشاء نشده ·

(Windows Server Service) MS08-067 انتشار با استفاده از آسیب*پذیری افشاء نشده ·

.در ادامه، هر یک از این زیرکلاس*ها با جزئیات بیشتری تشریح می*شود

ارتباطات همتا به همتا ·

کار می*کند. پس* از آلوده*سازی یک کامپیوتر، این مخاطرهRPC مولفه همتا به همتا با استفاده از نصب یک کارگزار و کارفرمای متصل شده و RPC را اجرا کرده و ارتباطات گوش می*دهد. تمامی کامپیوترهای آلوده شده می*توانند به این کارگزارRPC کارگزار .از نسخه استاکس*نت نصب شده روی کامپیوتر راه دور مطلع شوند

در صورتی*که نسخه راه دور به*روز تر از نسخه نصب*شده روی این کامپیوتر باشد، درخواستی مبنی بر دریافت نسخه جدیدتر ارسال شده، و استاکس*نت به*روزرسانی می*شود. در صورتی*که نسخه کامپیوتر راه دور قدیمی*تر باشد، یک کپی از مخاطره آماده شده، و به سیستم راه دور ارسال می*شود. با استفاده از این روش، امکان به*روز رسانی تمامی سیستم*های .آلوده فراهم شده، و این به*روزرسانی به تدریج در سطح شبکه پخش می*شود

:انجام می*شود RPC به*صورت زیر، با استفاده از P2P، تمامی درخواست*های

رویه**های زیر را در اختیار قرار می*دهد. (توجه داشته باشید که استاکس*نت از رویه*های 7، 8، و 9 استفادهRPC کارگزار .(نمی*کند

.نسخه استاکس*نت نصب*شده را باز می*گرداند :0 ·

(را دریافت و اجرا می*نماید (با استفاده از تزریقexe. یک فایل :1 ·

ماجول و اکسپورت اجرا شده را بارگذاری می*نماید :2 ·

و اجرای آن lsass.exe تزریق کد در :3 ·

.آخرین نسخه استاکس*نت را اجرا کرده، و آن را به کامپیوتر آلوده ارسال می*نماید :4 ·

ایجاد پردازه :5 ·

خواندن از فایل :6 ·

جاگذاری فایل : 7 ·

حذف فایل :8 ·

نوشتن رکوردهای داده :9 ·

1]>

شکل 8. مثالی از یک کارگزار قدیمی که نسخه جدید استاکس*نت را درخواست می*نماید

:درخواست*های زیر را ارسال می*نماید RPC کارفرمای

تابع 0را به*منظور دریافت نسخه سیستم راه دور فراخوانی می*نماید .1

بررسی می*کند که آیا نسخه راه*دور به*روز تر از نسخه محلی است .2

:در صورتی که نسخه راه دور به*روز تر باشد .3

تابع 4را به*منظور درخواست آخرین نسخه استاکس*نت فراخوانی می*نماید .a

آخرین نسخه را دریافت می*نماید .b

با استفاده از تزریق پردازه آن را نصب می*نماید .c

در صورتی که نسخه راه دور قدیمی*تر باشد .4

از استاکس*نت موجود تهیه می*شود exe. یک نسخه مجزای .a

این نسخه با استفاده از تابع 1 به سیستم راه دور ارسال می*شود .b

.راه دور این کلاس از فرآیند زیر استفاده می*نماید RPC به*منظور ارتباط با کارگزار

تابع 0 را روی هر کدام از موارد زیر، به*ترتیب، فراخوانی می*کند. در صورت موفقیت هر یک از فراخوانی*ها، استاکس*نت کار را ادامه می*دهد binding با استفاده از آن:

1. ncacn_ip_tcp:IPADDR[135]

2. ncacn_np:IPADDR[\\\\pipe\\\\ntsvcs]

3. ncacn_np:IPADDR[\\\\pipe\\\\browser]

زیر را امتحان می*کند binding در ادامه، این مخاطره یک توکن خاص را جعل کرده، و:

4. ncacn_np:IPADDR[\\\\pipe\\\\browser]

های دیگر می*گرددbinding به دنبال SCM (Service Control Manager) سپس به توکن خود رجوع کرده، و در:

5. ncacn_ip_tcp:IPADDR

پاسخ مناسب دهد، استاکس نت یک سیستم آلوده را پیدا کردهRPC های بالا به تابع 0 مربوط بهbinding در صورتی که هر کدام از است. تابع 0 نسخه استاکس*نت سیستم آلوده راه دور را باز می*گرداند. با توجه به این نسخه، استاکس*نت نسخه جدید را از .سیستم راه دور دریافت کرده، و یا نسخه خود را به سیستم راه دور ارسال می*نماید

شماره 1 به منظور دریافت آخرین نسخه از سیستم راه دور، و از تابع شماره 4 به منظور ارسال آخرین نسخهRPC از تابع .استاکس*نت استفاده می*شود

استاکس*نت نسخه قابل اجرای دریافت شده را به سادگی اجرا نمی*کند. در حقیقت، آن را در یک پردازه تزریق کرده و .به*صورتی که در بخش \"تکنیک تزریق\" بیان شد آن را اجرا می*نماید

است. در نتیجه، به*منظور ارسال یک نسخه اجرایی، استاکس*نت می*باید dll. علاوه بر این، استاکس*نت در حقیقت یک فایل را از منبع 210 خوانده، و آن راtemplate.exe یک نسخه اجرایی از خود را ایجاد نماید. بدین منظور، استاکس*نت در ابتدا یک فایل .با داده*های مورد نیاز به*منظور ایجاد یک نسخه اجرایی به*روز شده پر می*کند

کار می*کند، نمی*تواند به عنوان روشی جایگزین برای فرمان و کنترل RPC از آنجا که مکانیزم همتا به همتا با استفاده از قابل استفاده است. هدف از استفاده از روش همتا به همتا، فراهم آوردن دسترسی بهLAN استفاده شود، چرا که در یک کامپیوترهایی است که دسترسی به اینترنت نداشته، اما قابلیت ارتباط با دیگر کامپیوترهای موجود در شبکه محلی (که به .دسترسی دارند) را دارا می*باشندC&C کارگزار

WinCC آلوده*سازی کامپیوترهای ·

را اجرا می*نماید.* در صورت پیدا کردن سیستمی که اینWinCC این کلاس مسؤول ارتباط با کارگزار راه دوری است که نرم*افزار کد شده، به کارگزار پایگاه داده*ها متصلWinCC نرم*افزار را اجرا می*نماید، با استفاده از گذرواژه*ای که در نرم*افزار را به پایگاه داده*ها ارسال SQL می*شود. پس از برقراری ارتباط، دو عمل انجام می*شود. در ابتدا، استاکس*نت کدهای بدخواه را اجرا می*نماید. در ادامه، WinCC می*نماید، که این امر منجر به انتقال نسخه*ای از استاکس*نت به کامپیوتری می*شود که استاکس*نت یکی از دید*های جاری را تغییر داده، و کدی را به آن اضافه می*نماید که در هر بار دسترسی به دید اجرا .می*شود

را ارسال می*کند که جدولی را ایجاد کرده، و یک SQL استاکس*نت یک عبارت ،SQL پس از ارسال یک پرس*و*جوی پیکربندی اصلی استاکس*نت در قالب یک فایل DLL (مقدار باینری را در آن وارد می*کند. این مقدار باینری نمایش رشته*ای (مبنای 16 .اجرایی است

CREATE TABLE sysbinlog (abin image) INSERT INTO sysbinlog VALUES(0x…)

خودش را از پایگاه داده*ها روی دیسک، OLE Automation Stored Procedures در صورت موفقیت، استاکس*نت با استفاده از .می*نویسد ،%UserProfile%\\sql[RANDOM VALUE].dbi تحت عنوان

.این فایل، در ادامه، به*صورت یک رویه ذخیره شده اضافه شده، و اجرا می*شود

SET @ainf = @aind '\\\\sqlx.dbi'

EXEC sp_addextendedproc sp_dumpdbilog, @ainf

EXEC sp_dumpdbilog

.اصلی نیز حذف می*شودDLL این رویه ذخیره شده، حذف شده و فایل

را از منبع cab203. است اجرا شود، یک فایل WinCC در صورتی که استاکس*نت به*صورت محلی روی کامپیوتری که شامل اصلی استاکس*نت را از DLL است که DDL شامل یک cab. ذخیره می*نماید. این فایلGracS\\cc_tlg7.sav گرفته و با عنوان بارگذاری می*نماید. سپس، یک دید را به*منظور بارگذاری مجدد خود تغییر می*دهد. استاکس*نت دید GracS\\cc_alg.sav بیشتر، تغییر می*دهد. این کد SQL برای اجرای کدهای ،syscommnets.text را به منظور تجزیه فیلدMCPVREADVARPERCON .و –*ذخیره می*شود CC-SP– بین دو علامت syscomments.text ذخیره شده در

می*شود، (xp_cmdshell با استفاده از) cab. ی را که منجر به اجرای استاکس*نت از فایلSQL در حقیقت، استاکس*نت کد .ذخیره و اجرا می*نماید

set @t=left(@t,len(@t)-charindex('\\\\',reverse(@t))) '\\GraCS\\cc_tlg7 .sav';

set @s = 'master..xp_cmdshell ''extrac32 /y "' @t '" "' @t 'x"""';

```
exec(@s);
```

باز شده به عنوان یک رویه ذخیره شده اضافه شده، اجرا، و حذف می*شود. این امر به استاکس*نت اجازهDLL ،سپس .می*دهد که خود را اجرا کرده، و اطمینان حاصل نماید که مقیم باقی می*ماند

انتقال با استفاده از به*اشتراک*گذاری*های شبکه ·

در اشتراک*گذاری*های شبکه پخش [2] WMI استاکس*نت همچنین می*تواند با استفاده از کارهای برنامه*ریزی شده[1] و یا .شود

.استاکس*نت تمامی حساب*های کاربری کامپیوتر و دامنه، و تمامی منابع شبکه را بررسی می*کند

دسترس*پذیر است. با استفاده از $ADMIN استاکس*نت، به*منظور ایجاد نام اشتراکی درایو اصلی، بررسی می*کند که آیا اصلی و اخیرترین داده*های پیکربند، یک فایل اجرایی ایجاد می*شود. پس از بررسی تمامیDLL منبع 210، و با استفاده از کد کپی می*شود. سپس،DEFRAG[RANDLNT].tmp دایرکتوری*های شبکه، این فایل اجرایی به*صورت یک فایل تصادفی در قالب .یک کار شبکه، به منظور اجرای فایل، 2 دقیقه پس از آلوده*سازی، برنامه*ریزی می*شود

MS10-061 (Print Spooler) آسیب*پذیری افشاء نشده ·

منتشر شده است. اگر چه در ابتدا تصور می*شد MS10-061 توسط مایکروسافت در Print Spooler وصله مربوط به آسیب*پذیری منتشر شده بوده، و از آن زمانHakin9 که این آسیب*پذیری محرمانه بوده، ولی بعدا مشخص شد که نسخه 2009-4 مجله .عمومی بوده است. اما استفاده*ای در سطح گسترده نداشته است

ماشین آسیب*پذیر نوشته شود. کد انجام این عمل در %System% این آسیب*پذیری اجازه می*دهد که یک فایل در شاخه ذخیره شده در منبع مذکور را بارگذاری کرده، و پارامترهای مورد نیاز برای انجامDLL منبع 222 ذخیره می*شود؛ این اکسپورت بارگذاری شده فراخوانی DLL و یک کپی از کرم*واره، را آماده می*سازد. در ادامه اکسپورت یک از IP حمله، مثل آدرس کامپیوترهای مقصد کپی کرده، و سپسsystem می*شود. با استفاده از این اطلاعات، استاکس*نت می*تواند خود را در شاخه .خود را اجرا نماید

استفاده می*کند که تاریخ کنونی سیستم پیش از 1 ژوئن 2011 MS10-061 استاکس*نت تنها در صورتی از آسیب*پذیری .باشد

MS08-067 (Windows Server Service) آسیب*پذیری ·

نیز استفاده شده W32.Downadup نیز استفاده می*کند. این آسیب*پذیری توسط MS08-067 استاکس*نت از آسیب*پذیری و ارسال یک رشته مسیر ساختگی امکان*پذیر است. استاکس*نت با SMB است. سوء استفاده از این آسیب*پذیری با اتصال به .استفاده از این آسیب*پذیری خود را در سیستم*های به*روزرسانی نشده کپی* می*کند

:شرایط زیر را بررسی می*کند ،MS08-067 استاکس*نت، پیش از سوء استفاده از

.تاریخ کنونی باید پیش از 1 ژانویه 2030 باشد ·

.تعاریف آنتی*ویروس*ها پیش از 1 ژانویه 2009 باشد ·

(پیش از 12 اکتبر 2008 باشد (پیش از تاریخ وصله Netapi.dll و Kernel32.dll تاریخ ·

انتشار از طریق*های درایو*های قابل انتقال ·

یکی از روش*های اصلی مورد استفاده توسط استاکس*نت برای انتشار، کپی خود در درایوهای قابل انتقال است.
سیستم*های کنترل صنعتی معمولا با یک کامپیوتر ویندوزی برنامه*ریزی می*شوند، که به شبکه متصل نبوده، و کاربران معمولا داده*ها را با استفاده از درایوهای قابل انتقال منتقل می*نمایند. استاکس*نت از دو روش به*منظور انتشار به/از درایو*های قابل :انتقال استفاده می*کند

.استفاده از یک آسیب*پذیری که با مشاهده یک درایو قابل انتقال، امکان اجرای خودکار را فراهم می*آورد .1

autorun.inf استفاده از یک فایل .2

LNK (CVE-2010-2568) آسیب*پذیری ·

استاکس*نت خود و فایل*های پشتیبان خود را با ورود یک درایو قابل انتقال کپی می*نماید. این عمل با استفاده از اکسپورت*های 1، 9، و 32 پیاده*سازی شده است. اکسپورت 19 با استفاده از یک قطعه کد فراخوانی شده، و پس از آن روتین کپی توسط این اکسپورت انجام می*شود. اکسپورت*های 1 و 32 منجر می*شوند که روتین کپی تا زمان ورود یک درایو منتظر بماند. اکسپورتی که منجر به کپی بدافزار به درایوها می*شود، آلودگی روی درایوها را نیز، بر مبنای یک مقدار پیکربندی که در بلوک پیکربندی ذخیره شده، پاک می*کند. شرایط مختلفی وجود دارد که باعث می*شود فایل*های یک درایو آلوده پاک شوند.
.به عنوان مثال، پس از اینکه یک درایو آلوده سه کامپیوتر را آلوده کرد، فایل*های درایو آلوده پاک می*شوند

اجرا می*شود، و services.exe در صورتی که از اکسپورت*های 1 و 32 استفاده شود، استاکس*نت بررسی می*کند که آیا در ایجاد شده که منتظر ورود یک درایو 'AFX64c313' همچنین نسخه ویندوز تعیین می*شود. سپس، یک پنجره جدید مخفی با نام منطقی است (دارای نوعvolume قابل انتقال می*شود. در ادامه، بررسی می*شود که درایو شامل یک
.است). پیش از آلوده*سازی این درایو، تاریخ کنونی می*باید پیش از 24 ژوئن 2012 باشدDBT_DEVTYP_VOLUME

در ادامه، استاکس*نت اسم درایو جدید را مشخص کرده، و با استفاده از داده*های پیکربندی تعیین می*کند که خود را پاک کند :و یا درایو را آلوده سازد. به*منظور انجام عمل پاک*سازی، فایل*های زیر حذف می*شود

%DriveLetter%\\~WTR4132.tmp ·

%DriveLetter%\\~WTR4141.tmp ·

%DriveLetter%\\Copy of Shortcut to .lnk ·

- %DriveLetter%\\Copy of Copy of Shortcut to .lnk

- %DriveLetter%\\Copy of Copy of Copy of Shortcut to .lnk

- %DriveLetter%\\Copy of Copy of Copy of Copy of Shortcut to .lnk

:به*منظور انجام آلوده*سازی، وجود شرایط زیر در درایو مقصد بررسی می*شود

- .درایو در این لحظه آلوده نشده باشد که با استفاده از زمان کنونی بررسی می*شود

- پرچم پیکربندی مبنی بر آلوده*سازی درایوهای قابل انتقال مقداردهی شده باشد، در غیر این*صورت آلوده*سازی بر مبنای تاریخ انجام می*شود.

- آلودگی بیش از 21 روز قدیمی نباشد

- درایو مقصد حداقل 5 مگابایت جای خالی داشته باشد

- درایو مقصد حداقل شامل 3 فایل باشد

:در صورتی*که این شرایط برقرار باشد، فایل*های زیر ایجاد می*شود

- در بر دارد و از منبع stub 210 اصلی استاکس*نت را در بخش DLL این فایل) (~500Kb) %DriveLetter%\\~WTR4132.tmp (به*دست می*آید)

- را فراخوانی کرده و با استفاده از منبع 241 به*دست ~WTR4141.tmp این فایل) (~25Kb) %DriveLetter%\\~WTR4141.tmp (می*آید)

- %DriveLetter%\\Copy of Shortcut to .lnk

- %DriveLetter%\\Copy of Copy of Shortcut to .lnk

- %DriveLetter%\\Copy of Copy of Copy of Shortcut to .lnk

- %DriveLetter%\\Copy of Copy of Copy of Copy of Shortcut to .lnk

با استفاده از منبع 240 ایجاد می*شوند. از آنجا که هر یک از آنها یک (یا بیشتر) نسخه مختلف از ویندوز (شامل.lnk فایل*های را هدف قرار می*دهد، به حداقل 4تا (Windows 7 و Windows Vista، Windows XP، Windows Server 2003، Windows 2000 را، در صورت مشاهده پوشه، ~WTR4141.tmp شامل اکسپلویتی است که به*صورت خودکار.lnk از آنها نیاز داریم. فایل*های .اجرا می*نماید

را بارگذاری می*کند، اما پیش از این، فایل*های خود روی درایو مقصد را مخفی WTR4132.tmp~ سپس WTR4141.tmp~ می*نماید. از آنجا که کارکرد روت*کیت این بدافزار هنوز فعال نشده، مخفی*سازی در زودترین زمان ممکن، از اهمیت بالایی .تکنیک خاص خودش را در این زمان پیاده*سازی می*نماید WTR4141.tmp~ ،برخوردار است. در نتیجه

:استفاده می*کند (Ntdll.dll و kernel32.dll های زیر (مربوط بهAPI ازWTR4141.tmp~

:Kernel32.dll از

· FindFirstFileW

· FindNextFileW

· FindFirstFileExW

:Ntdll.dll از

· NtQueryDirectoryFile

· ZwQueryDirectoryFile

:این بدافزار کد اصلی این توابع را با کدی که به*دنبال فایل*هایی با خواص زیر می*گردد جایگزین می*نماید

.که سایزی معادل 4،171 بایت دارند lnk. فایل*هایی با پسوند ·

:xxxx است. منظور ازMBو 8 kbکه سایز آنها بین 4 ،WTRxxxx.TMP~ فایل*هایی با نام ·

اعداد 4 رقمی o

مجموع این اعداد بر 10 بخش*پذیر است o

ها به*گونه*ای تغییر می*یابد کهAPI در صورتی که در خواستی مبنی بر نمایش یک فایل با مشخصات بالا ارسال شد، پاسخ این .بیان*گر این مطلب باشد که فایل وجود ندارد. در نتیجه، تمامی فایل*ها با این ویژگی مخفی می*شوند

،به*صورت عادی، یک برنامهdll. بارگذاری می*شود. به*منظور بارگذاری یک فایل WTR4132.tmp~ ،هاAPI پس از استفاده از ی که باید در حافظه بارگذاری شود، فراخوانی می*نماید. استاکس*نت از روش دیگری،dll. را با نام فایل "\Load Library\" API .ها\" توضیح داده می*شود استفاده می*نمایدDLL که در بخش \"عبور از بلوکه*سازی مبتنی بر رفتار هنگام بارگذاری

DLL است. این فایل در حافظه بازگشایی شده، و اکسپورت stub15. اصلی استاکس*نت در بخش DLL شامل WTR4132.tmp~ .فراخوانی می*شود که نصب استاکس*نت را انجام می*دهد. اکسپورت 15 در بخش نصب توضیح داده می*شود

.شکل 9جریان اجرا را نمایش می*دهد

1]> <

شکل 9. جریان اجرا روی درایوهای قابل انتقال

Autorun.inf ·

پخشautorun.inf استفاده نمی*کردند، بلکه با استفاده از یک فایل LNK نسخه*های قبلی استاکس*نت از آسیب*پذیری می*شدند. منبع 207 یک فایل 500 کیلوبایتی است که در نسخه*های قبلی استاکس*نت وجود داشته، ولی در نسخه جدید .حذف شده است

یک فایل پیکربندی است که روی درایوهای قابل انتقال قرار داده شده، و با وارد کردن درایو، منجر به اجرای autorun.inf یک فایل و فایل اجرایی در ریشه درایو قرار داده می*شود. اما استاکس*نت از یک autorun.inf فایل*های دلخواه می*شود. معمولاً، فایل .با قالب مشخص قرار داردautorun.inf فایل استفاده می*نماید. منبع 207 یک فایل اجرایی است که در انتهای آن یک فایل

توسط ویندوز، از کاراکترهایی که به*عنوان دستورات مجاز شناخته نمی*شوند، autorun.inf هنگام تجزیه فایل*های قرار autorun.inf را در ابتدای فایل MZ چشم*پوشی می*شود. استاکس*نت از این نقصان به نفع خود استفاده نموده، و فایل را در ادامه مشاهدهautorun.inf چشم*پوشی می*شود. سرآیند و پی*آیند فایل MZ می*دهد. در روند تجزیه، از تمامی فایل :می*نمایید

1]> <

autorun.inf شکل 10. سرآیند

1]> <

autorun.inf شکل 11. پی*آیند

:اگر تنها رشته*های پی*آیند را در نظر بگیریم، می*بینیم که از دستورات مجازی تشکیل شده*اند

1]> <

autorun.inf شکل 12. دستورات مجاز در پی*آیند فایل

به*منظور مشخص کردن فایل اجرایی به عنوان فایل اصلی autorun توجه داشته باشید که استاکس*نت از دستورات در ابتدا، به*عنوان یک فایل مجاز، و در ادامه ،autorun.inf استفاده می*نماید. با استفاده از این روش، فایل autorun.inf .به*عنوان یک فایل اجرایی شناخته می*شود

علاوه بر این، استاکس*نت از یک روش دیگر نیز به*منظور بالا بردن احتمال اجرای خود استفاده می*نماید. دستورات اتوران، اجرای خودکار را غیر فعال ساخته، و دستور جدیدی را به منو اضافه می*کنند. دستور جدید را می*توان در است. در نتیجه، دو دستور "\Open"\ مشاهده نمود. در حقیقت این دستور همان %Windir%\\System32\\shell32.dll,-8496

.در منو مشاهده می*شودOpen

1]> <

جدید Open شکل 13. اضافه شدن یک دستور

دستور مجاز و دیگری غیرمجاز است. اگر کاربر درایو مورد نظر را با این دستور باز کند، پیش از Open یکی از این دستورات .بازگشایی، استاکس*نت اجرا می*شود و در ادامه درایو مورد نظر باز می*شود

Step7 آلوده*سازی فایل*های پروژه ·

های خاص به*منظور باز کردن فایل*های پروژه درAPI اکسپورت اصلی، اکسپورت 16، اکسپورت 2 را فراخوانی می*نماید، که از بوده، و از آن به**منظور مدیریت پروژه WinCC Simatic استفاده می*نماید. این پردازه، مدیر s7tgtopx.exe پردازه .استفاده می*شودWinCC/Step7

:های زیر تغییر داده می*شودDLL جداول آدرس مربوط به

به*گونه*ای تغییر می**یابد که به CreateFileA آدرس ،msvcrt.dll و ،mfc42.dll ،s7apromx.dll های dllدر ·
.اشاره نماید "\CreateFileA_hook\"

.اشاره نمایدStgOpenStorage_hook"\ به*گونه*ای تغییر می*یابد که بهStgOpenStorage ،ccprojectmgr.exe در ·

CreateFileA_hook ،استفاده می*شود. در عوض (Step7 فایل*های پروژه) S7P.* به*منظور بازکردن پروژه*های CreateFileA از را فراخوانی RPC تابع شماره CreateFileA_hook 9 ،باشد s7p. فراخوانی می*شود. در صورتی*که پسوند فایل بازگشایی شده ذخیره نموده، و پوشه*ای که این فایل درoem6c.pnf%Windir%\\inf\\ می*کند، که مسیر کنونی را در فایل داده*ای رمزشده .آن قرار دارد را آلوده می*سازد

Step7 استفاده می*نماید. این فایل*ها در پروژه*هایMCP. به*منظور باز کردن فایل*های StgOprnStorage از Simatic مدیر نظارت دارد. در صورت دسترسی به چنینmcp. بر فایل*هایی با پسوندStgOpenStorage_hook، CreateFileA وجود دارد. همانند در آن قرار mcp فراخوانی شده، و پوشه پروژه*ای که فایلoem6c.pnf به*منظور ذخیره*سازی مسیر RPC فایلی، تابع شماره 9 .دارد فراخوانی می*شود

.استStep7 اکسپورت 14 روتین اصلی آلوده*سازی فایل*های پروژه

روتین آلوده*سازی پروژه مسیر یک پروژه را به*عنوان ورودی دریافت کرده، و با اجرای استاکس*نت هنگام بارگذاری پروژه، آن را .آلوده می*سازد

.انجام می*شود mcp. یا ،s7p. ،tmp. فایل*های داخل پروژه لیست می*شود. پردازش ویژه*ای روی فایل*ها با پسوند

S7P فایل*های ·

هستند. در صورتی که چنین فایلی در پوشه پروژه قرار داشته باشد، پروژه Step7 فایل*هایی با این پسوند، فایل*های پروژه .ممکن است آلوده باشد

:پروژه می*تواند آلوده شود، در صورتی*که

(بیش از حد قدیمی نباشد (در 3.5 سال گذشته استفاده شده باشد ·

مجاز باشدMCP با یک فایل "\wincproj"\ شامل پوشه*ای با نام ·

.انجام می*شود "\Step7\\Examples*"\ نمونه نباشد. این امر با حذف مسیرهای Step7 یک پروژه ·

:رویه آلوده*سازی شامل گام*های متفاوت مختلفی است

:استاکس*نت فایل*های زیر را ایجاد می*نماید .1

(استاکس*نت اصلی DLL یک کپی رمزشده از) a. xutils\\listen\\xr000000.mdx

(یک نسخه از فایل داده*ای استاکس*نت که طولی معادل 90 بایت دارد) b. xutils\\links\\s7p00001.dbf

(یک نسخه رمزشده و به*روزشده از بلوک داده*های پیکربندی استاکس*نت) c. xutils\\listen\\s7000001.mdx

ی که در منبعDLL را بررسی می*نماید. استاکس*نت در هر یک از آنها یک کپی از "\hOmSave7"\ این مخاطره زیرپوشه*های .2 .با استفاده از نام فایل خاص کپی می*شودDLL 202 وجود دارد را کپی* می*نماید. این

.قرار دارد تغییر می*دهد Apilog\\types را که درStep7 استاکس*نت فایل داده*ای .3

از آن استفاده شد DLL پس از اینکه یک پروژه آلوده شده باز شد، فایل داده*ای تغییر یافته به دنبال نام فایلی که برای کپی :می*گردد. پوشه*های زیر به ترتیبی که در ادامه می*آید جستجو می*شوند

Step7 از پوشه نصبS7BIN پوشه ·

%System% پوشه ·

%Windir%\\system پوشه ·

%Windir% پوشه ·

hOmSave7 زیرپوشه*های پوشه ·

dll. بدخواه توسط مدیر بارگذاری و اجرا می*شود. این فایلDLL ،در صورتی*که فایل مذکور در هیچ*یک از 4 پوشه بالا پیدا نشد قرار دارد عمل می*نماید. این استراتژی مشابه xutils\\listen\\xr000000.mdx اصلی که درdll به*عنوان رمزگشا و بارگذار کپی حملات DLL Preloading است.

نسخه*های 5.3 و 5.4 (بسته خدماتی 4) قابلیت آلوده*شدن را دارا می*باشند. اما از آسیب*پذیر بودن نسخه*های اخیر مدیر اطلاعی در دست نیست (v5.5 و v5.4 SP5).

· فایل*های MCP

ایجادWinCC وجود دارند. اما، به*صورت معمول توسط Step7 نیز در پوشه پروژه mcp. فایل*های ،s7p. مشابه فایل*های آلوده بودن پروژه را نیز ،WinCC می*شوند. پیدا کردن چنین فایلی در یک پروژه می*تواند, علاوه بر آلوده بودن پایگاه داده*های القاء نماید.

پروژه می*تواند آلوده باشد اگر:

· (بیش از حد قدیمی نباشد (در 3.5 سال اخیر دسترسی به آن انجام شده باشد

· باشد pdl. با حداقل یک فایل GracS شامل یک پوشه

روند آلوده*سازی شامل گام*های مختلفی خواهد بود:

1. استاکس*نت فایل*های زیر را ایجاد می*نماید:

a. GracS\\cc_alg.sav (استاکس*نت اصلی DLL یک نسخه رمزشده از)

b. GracS\\db_log.sav (یک کپی از فایل داده*ای استاکس*نت به طول 90 بایت)

c. GracS\\cc_alg.sav xutils\\listen\\s7000001.mdx (یک نسخه رمز شده و به*روز شده از بلوک داده پیکربندی استاکس*نت)

2. سپس یک نسخه از منبع 203 رمزگشایی شده و در GracS\\cc_tlg7.savفایل یک این فایل. شود*می قرار داده Cabinet
ویندوز است که به*منظور بارگذاری و اجرای استاکس*نت از آن استفاده می*شود.

ممکن است مورد دسترسی قرار گرفته، و آلودگی به ماشین کارگزار پایگاهWinCC در فرآیند آلوده*سازی، پایگاه داده*های منتقل شود. این رویه در بخش \"پخش در شبکه\" تشریح خواهد شد WinCC داده*های.

· فایل*های TMP

که در پروژه وجود دارد، نام فایل در ابتدا بررسی می*شود. قالب این نام باید به*صورت tmp. به*ازای هر فایل ،اعدادی در مبنای 16 هستند که مجموع آنها بر 16 بخش*پذیر است. به*عنوان مثال "\xxxxx\" باشد کهWRxxxxx.tmp~ نامی مجاز است WR12346~.

باشد. در این*صورت، مابقی داده "\LRW~LRW~\" در ادامه محتویات فایل بررسی می*شود. 8 بایت اولیه *باید شامل رشته رمزگذاری می*شود.

استاکس*نت می*تواند با استفاده از پروژه*های آلوده شده خود را به*روزرسانی نماید. در صورتی که یک پروژه باز شده و آلوده باشد، استاکس*نت نسخه آلودگی را بررسی کرده، و در صورتی*که این نسخه جدیدتر باشد، آن را به*منظور به*روزرسانی خود اجرا می*نماید.

سه فرم متفاوت از فایل*های پروژه آلوده وجود دارد که هر کدام توسط یک اکسپورت خاص مدیریت می*شود.

را به*عنوان ورودی می*گیرد. در ادامه مسیرهای مربوط به فایل*های زیر درون پروژه ایجاد Step7 اکسپورت 9 مسیر یک پروژه می*شود:

- ...\\XUTILS\\listen\\XR000000.MDX
- ...\\XUTILS\\links\\S7P00001.DBF
- ...\\XUTILS\\listen\\S7000001.MDX

اضافه شده، و اکسپورت 16، نقطه ورود اصلی در این نسخه (%Temp%\\~dfXXXX.tmp) این فایل*ها به فایل*های موقت به*روزتر استاکس*نت، اجرا می*شود.

را به*عنوان وروی گرفته، و مسیر*های مربوط به فایل*های استاکس*نت زیر که در پروژه Step7 اکسپورت 31 یک مسیر پروژه قرار دارند را ایجاد می*نماید:

- ...\\GracS\\cc_alg.sav
- ...\\GracS\\db_log.sav
- ...\\GracS\\cc_tag.sav

- اضافه شده، و اکسپورت 16، نقطه ورود اصلی در این نسخه (%Temp%\\~dfXXXX.tmp) این فایل*ها به فایل*های موقت به*روزتر استاکس*نت، اجرا می*شود.

را پردازش کرده، و فایل*های Step7 اکسپورت 10 مشابه اکسپورت*های 9 و 31 می*باشد. این اکسپورت می*تواند پوشه*های Zip نیز مورد قرار دارند را استخراج نماید. حتی ممکن است آرشیو*های \\Xutils و \\Gracs استاکس*نتی که در زیرپوشه*های پردازش قرار گیرند.

از اکسپورت 16 به*منظور اجرای نسخه استخراج*شده از استاکس*نت استفاده شده، و بلوک داده*های پیکربندی به*روز می*شود.