از جنجال خبری تا واقعیت:

Narilam بدافزار سال 2010

چند روز پیش کمپانی سیمانتک گزارش پرحاشیه‌ای مبنی بر کشف یک بدافزار جدید با نام Narilamرا منتشر کـرد و اعلام داشت این بدافزار جهت حمله به سرورهای ایرانی طراحی شده است. اما بررسی‌هـای کسپرسـکی نگـاه کـاملا متفاوتی به این بدافزار دارد.

پس از انتشار این خبر کسپرسکی اعلام کرد که نگارش‌های اول این بدافزار در سال‌های 2010 و 2011 توسط ایـن شرکت کشف و پاکسازی شده است و از آنجا که در چند ماه اخیر در جهان تنها شش مورد از بدافزار نامبرده گـزارش شده، می‌توان گفت که دیگر عمر خطر آن به سر رسیده باشد.

همچنین با بررسی‌های انجام شده معلوم شد که هدف ناریلام آسیب رساندن به برخی از پایگاه هـای داده محصـولات شرکت "طراح سیستم" است. دست آخر هم اینکه هنوز هیچ مدرکی دال بر ارتباط این بدافزار با بدافزارهای سـریالی Wiper، Stuxnet و Flame دیگر بدافزارهای شناخته شده مشابه یافت نشـده اسـت و بـا توجـه بـه روش برنامـه نویسی فعلا تمام شواهد نشان از تفاوت کلی و زیربنایی آنها دارد.

اما همین سوابق حملات سایبری و التهاب امنیتی فضای سایبری ایران به هرچه داغ تر شدن خبر منتشر شده توسط سیمانتک دامن زد تا آنجا که مرکز مدیریت امداد (ماهر) را وادار بـه انتشـار اطلاعیـه ای رسـمی کـرد. در مـتن ایـن اطلاعیه، ماهر به وضوح به کاربران اطمینان خاطر داد که در خصوص این بدافزار به نوعی "سوء تفاهم" پیش آمـده و موضوع مربوط به سال 2010 است و چند سال پیش کشف و پاکسازی آن انجام گرفته است.

اطلاعیه مرکز ماهر مهر تاییدی بود بر گزارش **کسپرسکی** مبنی بر اینکه اولین ویـرایش‌هـای ایـن بـدافزار در سـال 2009 تـا 2010 منتشـر شـده اسـت و کسپرسـکی چنـدین نسـخه آن را بـا نـام‌هـای گونـاگونی ماننـد Trojan.Win32.Scar.cvcwدر سال 2010، یا Trojan.Win32.Scar.dlvc در سال 2011 کشف کرده و نیز برخـی از ویـرایش‌هـای جدیـد ایـن بـدافزار توسـط سیسـتم هوشـمند کشـف بـدافزار **کسپرسـکی** بـا نـام HEUR:Trojan.Win32.Generic کشف می‌شوند.

روی هم رفته تا کنون چندین ویرایش از این بدافزار توسط **کسپرسکی** کشف شده است که همه آنها سایزی حدود 1.5MB را دارند و همگی بر روی سیستم عامل Windows اجرا می‌شوند. اگر چنانچه به Header کامپایلر آن که Borlan C++ است اعتماد کنیم، مشهود است که تاریخ ساخت و انتشار آن به سال‌های 2009 تا 2010 بازمی‌گردد:

Count of sections	8	Machine	intel386
Symbol table 00000000[00000000]		Thu Sep 03 19:21:05 2009	
Size of optional header	00E0	Magic optional header	010B
Linker version	5.00	OS version	4.00
Image version	0.00	Subsystem version	4.00
Entry point	00001410	Size of code	000C6000
Size of init data	00092000	Size of uninit data	00000000
Size of image	00198000	Size of header	00000600
Base of code	00001000	Base of data	000C7000
Image base	00400000	Subsystem	Windows GUI
Section alignment	00001000	File alignment	00000200
Stack	00100000/00002000	Heap	00100000/00001000
Checksum	00198EB2	Number of directories	16

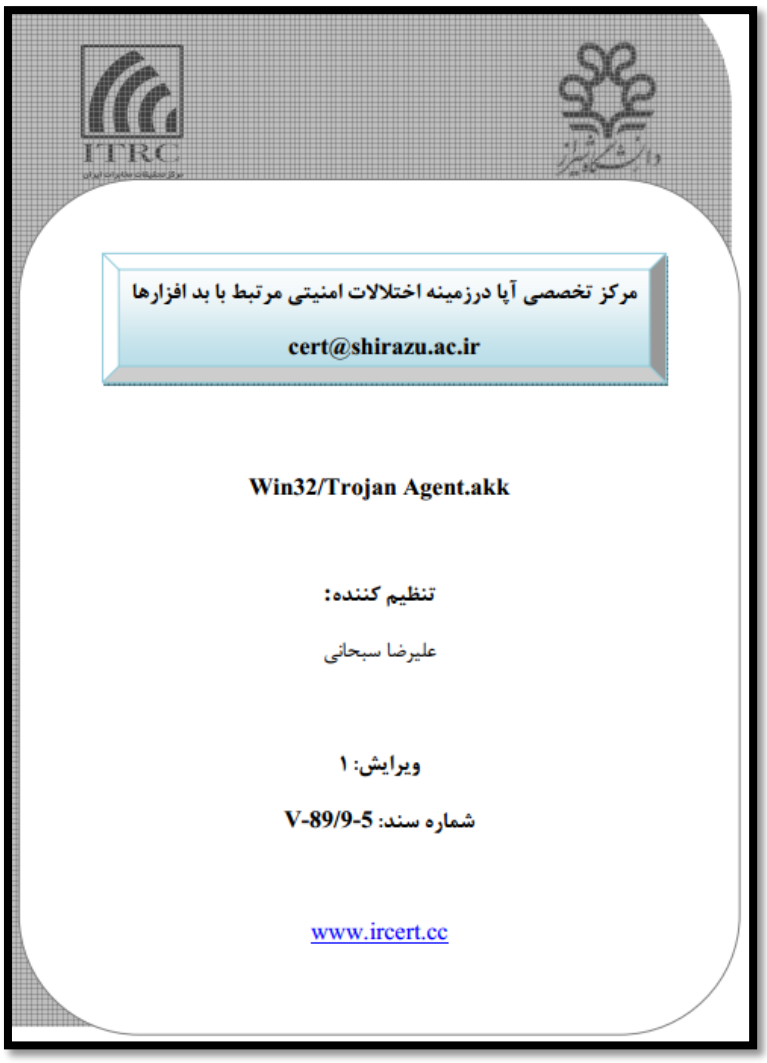
بررسی شباهت با Wiper، Stuxnet، Duqu یا Flame

پس از گزارش سیمانتک، اولین نکته‌ای که به ذهن همگان خطور کرد، ارتباط Narilam با بدافزارهایی مانند Stuxnet و Flame و دیگر بدافزارهایی بود که در این دو سال اخیر در ایران منتشر شدند. براساس بررسی‌ها و آنالیز شرکت کسپرسکی، هیچ مدرک قابل استنادی دال بر ارتباط Narilam با Stuxnet، Duqu، Wiper، Flame و Gauss یافت نشد. چراکه بدافزارهای ذکر شده همگی با نسخه هایی از Visul C کامپایل شده‌اند در حالی که Narilam با Borland C++ Builder 6کامپایل شده که ابزار برنامه نویسی کاملا متفاوتی است.

به راستی عمر Narilam چقدر است؟

مانند همیشه، نشانه زمانی کامپایلر می‌تواند دروغین و دستکاری شده باشد. اما هشدارهای سال‌های گذشته که مربوط به همین بدافزار است، سندی است بر صحت این موضوع که چند سال از کشف بدافزار Narilam می‌گذرد. به عنوان مثال در سند زیر که در تاریخ 1389/9/28 (30/6/2010) توسط ارگان IRTC یا "آپا" (آگاهی رسانی، پشتیبانی و امداد در زمینه اختلالات امنیتی فضای رایانه‌ای) با شماره ارجاع VU-2000059منتشر شده ناریلام را 32/Trojan Agent.all نامیده است. این سند دلیلی است بر صحت تاریخ کشف ناریلام:

این تروجان خود را با یک هشدار خطای سیستمی بر روی صفحه اعلام می‌کند که مرورگر سیستم به وسیله ایـن تروجـان ربـوده شـده است ولازم است که یک ضدتروجان برروی سیستم نصب شود وگرنه سیستم دچار مشکل خواهد شـد. **این بـدافزار تغییراتـی را در جداول بانک‌های اطلاعاتی سیستم‌های جامع Amin, Maliran, Shahd و.... ایجاد می‌کند.**


مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

Win32/Trojan Agent.akk

تنظیم کننده:

علیرضا سبحانی

ویرایش: ۱

شماره سند: V-89/9-5

www.ircert.cc

علاوه بر این همانطور که بالاتر گفته شد، روز شنبه چهارم آذرماه (91/9/4) سازمان "ماهر" (مرکز مـدیریت امـداد و هماهنگی عملیات رخدادهای رایانه‌ای) بـا انتشـار اعلامیـه‌ای بـه شـماره IRCNE2012111683در سـایت خودبـه کاربران رسما اعلام می‌کند کـه W32.Narilamدر سـال 89 (2010) شناسـایی و گـزارش شـده، آن را بـدافزاری آماتور خطاب کرده و موضوع را بیشتر یک سوء تفاهم می‌داند.

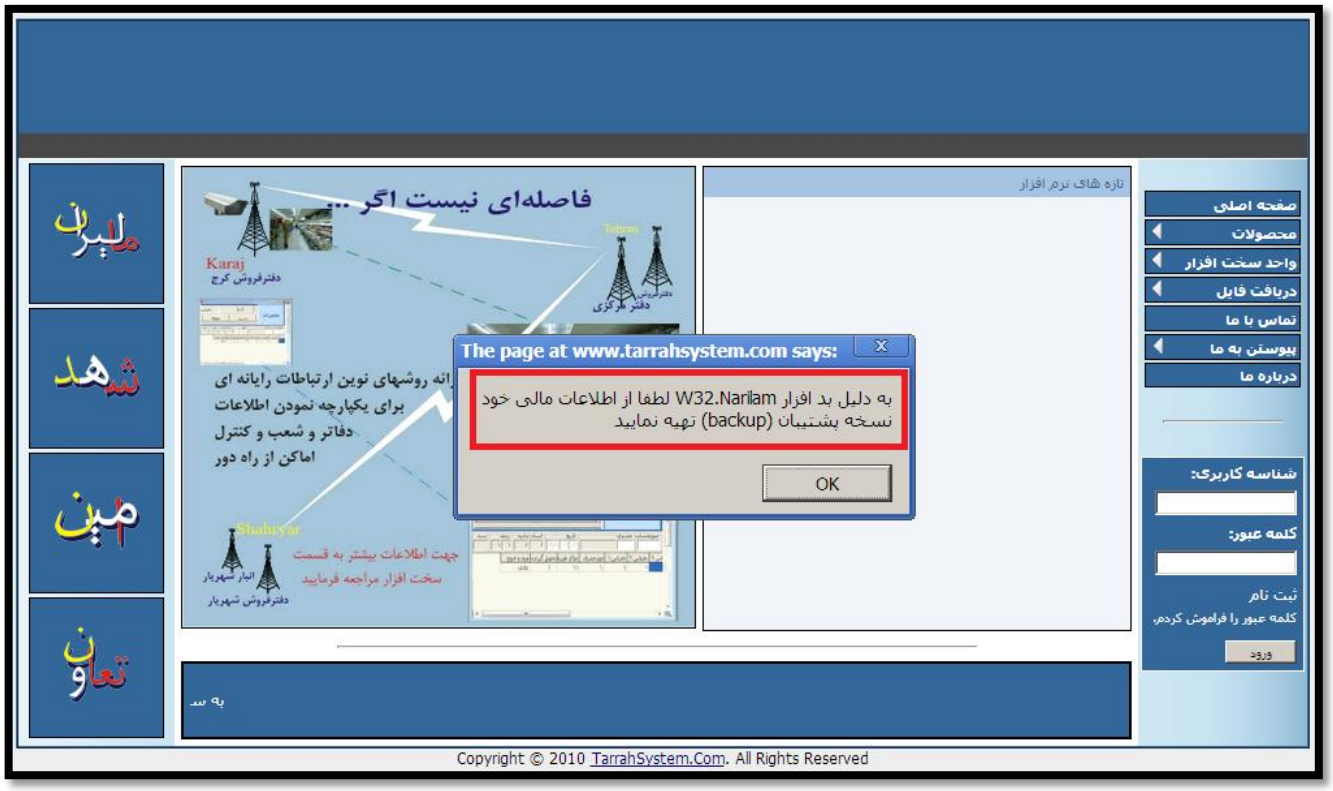
بدافزاری با هدف مشخص

همانطور که سیمانتک در گزارش خود گفته، این بدافزار دیتابیس‌های خیلی خاصی با نام‌هـای maliran، shahd و amin را هدف قرار می‌دهد و از برخی جدول‌های آنهـا ماننـد A_Sellers و Koll و Moein بـه صـورت تصـادفی اطلاعاتی را پاک می‌کند:

```
delete from A_Sellers Where Cast(sellercod as int)=@SanadNo
delete from Koll Where Cast(Koll as int)=@SanadNo
delete from Moein Where Cast(Moein as int)=@SanadNo
delete from Tafsily Where Cast(Tafsily as int)=@SanadNo
delete from person Where Cast(code as int)=@SanadNo
delete from Vamghest  Where Cast(vamno as int)=@vamno and @dresid=dresid
delete from Kalamast Where Idx =@SanadNo
```

که می‌توان گفت این رفتار منحصرا برروی اطلاعات یک کمپانی و نرم افزار خیلی خاص و مشـخص مـی‌توانـد عمـل کند.

شنیده شده است که اخیرا شرکتی به نام "طراح سیسـتم" هشـداری را در بـاره بـدافزاری منتشـر کـرد کـه بـدافزار W32.Narilam برخی از نرم افزارهای این شرکت را هدف قرار داده است. جالب اینکـه نـرم‌افزارهـای Maliran و Amin که در بالا به آنها اشاره شد، از محصولات این شرکت هستند.



روی هم رفته می توان گفت که Narilam که پیشینه کشف آن به سال 2010 باز می‌گردد، تنها این سه محصول شرکت "طراح سیستم" را هدف قرار می‌داده است و انتظار بیشتری از آن نمی‌رود.

"خلاصــه"

- با استناد به نشانه زمانی کامپایلر Narilam، می توان گفت که این بدافزار بین سال‌های 2009 تا اواسط 2010 نوشته شده است.
- هدف آن تخریب داده‌های برخی جداول از پایگاه داده‌های نرم افزارهای Maliran، Amin و Shahd از محصولات شرکت طراح سیستم بوده است.
- مرکز ماهر رسما این موضوع را یک سوء تفاهم خوانده و تاریخ کشفNarilamرا سال 1389 (2010) اعلام کرده است.
- طبق آمارهای شبکه امنیتی کسپرسکی (Kaspersky Security Network)، تقریباً 60٪ از این بدافزار در ایران و حدود 40٪ آن در افغانستان یافت شده است.
- تا به حال سند موثقی دال بر ارتباط این بدافزار با بدافزارهای سریالی Wiper، Shamoon، Flame و... بدست نیامده است.
- در حال حاضر نه تنها زمان کشف نسخه های مختلف این بدافزار تمام شده، بلکه مدت زیادی از مرحله پاکسازی جهانی آن هم می‌گذرد، و در چند ماه گذشته تنها شش مورد از این بدافزار در دنیا مشاهده و کشف شده است.

نویسنده: فرزاد غفوریان - مدیر واحد امنیت شرکت پاد