امنیت اطلاعات

بولتن تحلیلی ■ شماره پنجم ■ بهار ۱۳۹۳

یادداشت

آمدن بهار همراه است با نو شدن و طبیعت اولین همراه آن است. ما نیز همراه با این سبزی و شادابی حرکت خود را ادامه می‌دهیم و با آوردن سینِ "سعی" بر سر سفره هفت‌سین امسالمان، امیدواریم سینِ "سلامتی در فضای مجازی" را بر سفره هفت سین سال نوی مشتریانمان قرار داده باشیم. آرزوی ما سالی سرشار از موفقیت و شادکامی برای شماست.

در این شماره می خوانید:

فرایند مقابله با بدافزار در پادویش

دنبال کردن بدافزار، برای برخی از بدافزارها که به دریافت فایل‌های مخرب جدید از سرورهای نامشخص می‌پردازند.

شبکه ابر کاربران، متشکل از فایل‌هایی است که کاربران آنتی‌ویروس با آن‌ها روبرو هستند و آنتی‌ویروس به آن‌ها مشکوک می‌شود و برای بررسی ارسال می‌کند

یکی از فعالیت‌های متداول در حوزه مقابله با بدافزار جمع‌آوری بدافزارها در برخی سایت‌های مشهور می‌باشد

در بررسی صحنه جرم، با دسترسی به سیستم مشتری، فایل‌های مشکوک را به ورودی سیستم می‌فرستند

تله عسل(honey pot) یک سیستم با اطلاعات کاذب است که برای شبیه‌سازی ارتباطات مجازی در شبکه استفاده می‌شود

از مکان‌های مناسب برای نظارت و شناسایی بدافزارهای جدید، دروازه‌ها، میل سرورها و...هستند

بانک اطلاعات بدافزار

تحلیل بدافزار و تولید امضا

سامانه‌های تحلیل خودکار و تولید امضا

تحلیل انسانی و تولید امضا

پایگاه امضا بدافزار

تولید و بروزرسانی پایگاه امضا

سرور بروزرسانی و مجوز

کاربران

تحلیل بدافزار Atrax توسط تیم تحلیل پادویش

Atrax سارق مجازی

بدافزار Atrax که با نام Spy.Win32.AtraxBot.a شناسایی می‌شود نمونه‌ای از سارقان مجازی است که در اواسط سال ۲۰۱۳ میلادی شناسایی شد. به طور کلی می‌توان گفت طراحی این بدافزار در ابتدا به منظور جمع آوری اطلاعات از سیستم قربانی و ارسال آن به سرورهای مورد نظرش در بستر شبکه‌ی TOR بوده است. قدم بعدی بدافزار اقدام به برقراری ارتباطات c&c برای دریافت اطلاعات و دستورات جدید است.

شبکه‌ی TOR (مخفف The Onion Router) نمونه‌ای از شبکه‌های مخفی است. طراحی این شبکه‌ها به گونه ایست که توانایی پنهان سازی شناسه‌ی فرستنده و گیرنده پیام و هم‌چنین محتوای آن را دارا می‌باشند؛ بنابراین در ارسال اطلاعات مثل نقاب عمل می‌کنند. هر پیام برای رسیدن به مقصد خود از سه node دیگر در شبکه که به صورت تصادفی انتخاب شده اند عبور می‌کند. اطلاعات به همراه مقصد اصلی و nodeهای میانی در مبدأ رمزنگاری می‌شوند. این رمزنگاری با دریافت کلید عمومی هر یک از nodeهای میانی صورت می‌گیرد. لایه‌های رمزنگاری به گونه‌ای قرار دارند که در هر مرحله تنها آدرس node بعدی و قبلی مشخص است. در آخرین node رمز گشایی پایانی صورت گرفته و متن اصلی به مقصد نهایی ارسال می‌شود. دلیل نام گذاری این شبکه هم به نام شبکه‌ی پیازی به دلیل استفاده از لایه‌های چندگانه‌ی رمزنگاری می‌باشد که هر لایه در یک مرحله رمزگشایی شده تا دستیابی به لایه‌ی بعدی امکان پذیر شود.

علائم آلودگی

۱- در حال اجرا بودن برنامه‌ی iexplore، google chrome، firefox، opera و یا safari در سیستم شما به طور مداوم و به صورت پنهان حتی زمانی که از آن‌ها استفاده نمی کنید.

۲- وجود پارامتری در مسیر رجیستری HKCU\Software\Windows\CurrentVersion\Run به نام "Microsoft Svchost" که محتوی آدرس فایلی اجرایی در مسیر Application Data در سیستم است. نام پارامتر عددی ۵رقمی است.

۳- وجود دو یا سه فایل با مشخصه‌ی سیستمی و پنهان در مسیر Application Data در سیستم شما که نام همگی آن‌ها به صورت عددی در قالب hex بوده و در ۱۶ رقم ابتدایی مشترک می‌باشند. برای مثال دارای پیشوند CDE97FA2BFC1631D یا CC250462B0857727.

۴- وجود فایلی اجرایی به صورت پنهان در مسیر Application Data در سیستم شما که نام آن عددی ۵ رقمی می‌باشد. نام این فایل با مقداری که در رجیستری بالا گفته شد برابر است.

شکل زیر نمونه‌ای از فایل‌های ایجاد شده در مسیر Application Data را بعد از اجرای بدافزار نشان می دهد.

30023.exe	1,245 KB	Application
CDE97FA2BFC1631D685B8E6...	256 KB	System file
CDE97FA2BFC1631DEE11054...	229 KB	System file
17216.exe	1,245 KB	Application
CC250462B08577273A04C62...	887 KB	System file
CC250462B0857727DD35376...	264 KB	System file
CC250462B0857727E1B3864...	241 KB	System file

تصویر۱- نمونه‌ای از فایل‌های ایجادشده در مسیر Application Data بعد از اجرای بدافزار

ماژول‌ها و توالی عملیات بدافزار

اجرای کلی فرآیند این بدافزار را می‌توان به چهار بخش عمده تقسیم کرد:

۱- دانلود و راه اندازی ماژول ابتدایی.

۲- کپی شدن ماژول ذکر شده در مسیر Application Data در سیستم و اجرای آن با استفاده از دستور CreateProcessInternalW.

۳- اجرای فایل همراه با تزریق شدن کد در پردازه‌ی explorer.exe.

۴- انجام بخشی از جمع آوری اطلاعات سیستمی توسط کد تزریق شده در explorer.exe و راه اندازی پروسه‌ی iexplore.exe و تزریق کد به آن و سپس اجرای برنامه.

۵- اجرای بخش کد نوشته شده برای استفاده از بستر شبکه‌ی TOR

برای ارتباط با سرورهای مورد نظر و ارسال و دریافت داده توسط کد تزریق شده در iexplore.exe
به جای برنامه‌ی iexplore.exe هریک از برنامه‌های google ،firefox opera ،chrome و safari هم می‌توانند مورد حمله قرار گیرند. توجه داشته باشید که در واقع این پردازه سرویس TOR را در سیستم راه اندازی کرده و سیستم شما را به یک سرویس گیرنده در شبکه‌ی TOR تبدیل می‌کند.

بخش اول

این بخش توسط چند downloader ساده اجرا می‌شود که فایل‌ها را از سرورهای مورد نظر دریافت کرده و آن‌ها را بعد از دریافت با دستور ShellExecute اجرا می‌کنند. تعدادی نمونه از این URLها در لیست زیر آمده است.

http://tan***su/bin.exe
http://download.Ku****service-paypal.com

بخش دوم

اولین کاری که در برنامه‌ی اجرا شده صورت می‌گیرد غیر فعال کردن اجرا در محیط های تحلیل خودکار است. این کار با دریافت پارامتر "ProductId" از مسیر رجیستری زیر صورت می‌گیرد:

HKLM\Software\Microsoft\Windows NT\CurrentVersion

این پارامتر مربوط به مشخصه‌ی سیستم عامل نصب شده در سیستم است که در حالت عادی قابل دسترسی مستقیم نمی‌باشد. بعد از دریافت این اطلاعات که سریالی ۲۱ رقمی می‌باشد مقایسه‌ای با ۵ مقدار از پیش تعیین شده صورت می‌گیرد. در صورتی که این مقایسه نتیجه‌ای مثبت داشته و Id سیستم با هر یک از این ۵ مقدار برابر باشد اجرای بدافزار متوقف خواهد شد. در شکل زیر این ۵ سریال را مشاهده می‌کنید.

"76487-640-1457236-23837"	Anubis
"76487-644-3177037-23510"	CWSandbox
"55274-640-2673064-23950"	JoeBox
"76497-640-6308873-23835"	Malwr Cuckoo Sandbox
"76487-640-1464517-23529"	Malwr Cuckoo Sandbox

تصویر۲- نمونه‌ای از سریال هایی که از پیش تعیین شده اند

همان طور که در شکل مشخص شده است این سریال‌ها مربوط به نرم افزارهای شبیه ساز و تحلیلگر خودکار سیستم می‌باشد که در این قسمت به عنوان Anti Forensics از این تکنیک استفاده شده است.
در مرحله‌ی بعد مسیر فایل اجرایی با مسیر Application Data مقایسه شده و در حالتی که فایل در این مسیر نباشد بدافزار خود را با مشخصه‌ی پنهان و با نامی که یک عدد ۵ رقمی رندوم است در Application Data کپی کرده و با دستور CreateProcessInternalW بار دیگر اجرا می‌کند.

بخش سوم

در این بخش سه عمل مهم صورت می‌گیرد: ابتدا کلیدی با نام "Microsoft Svchost" در مسیر رجیستری زیر که شامل برنامه‌های AutoRun سیستم است ساخته می‌شود.

HKCU\Software\Windows\CurrentVersion\Run

با مقداردهی این کلید با مسیر فایل اصلی بدافزار در Application Data برنامه‌ی مخرب در هر بار بالا آمدن سیستم بار دیگر اجرا خواهد شد.
سه فایل دیگر که با فرمت رمز شده هستند با مشخصه‌ی سیستمی و پنهان در مسیر Application Data ایجاد می‌شوند. نام این فایل‌ها اعدادی در قالب Hex بوده و همگی در ۱۶ رقم ابتدایی خود مشترک می‌باشند. برای مثال فایل‌های ایجاد شده توسط این بدافزار همگی دارای پیشوند CC250462B0857727 در نام خود می‌باشند. این فایل‌ها در واقع سه پلاگین هستند که به صورت رمز شده در مسیر گفته شده ایجاد می‌شوند و در زمان استفاده نیز با همان مشخصه رمزگشایی خواهند شد.
در قدم بعدی تزریق کد در پردازه‌ی EXPLORER.EXE صورت خواهد گرفت.
بخشی از اطلاعاتی که این برنامه از سیستم دریافت می‌کند شامل موارد زیر است:

- ProductId
- DigitalProductId
- MachineGuid

در بخشی از کد برنامه در صورت وجود فایل زیر آن را پاک می‌کند.

C:\Windows\system32\15773_ATRAX_BOT_27585

بخش چهارم

کد تزریق شده در EXPLORER.EXE دو وظیفه‌ی عمده بر عهده دارد:
۱- جمع آوری اطلاعات مهمی از سیستم قربانی و تلاش برای برقراری ارتباط با سرور مورد نظرش برای ارسال داده ها.
۲- راه اندازه‌ی پردازه‌ای با نام یکی از مرورگران وب موجود در سیستم و تزریق کدی برای آماده سازی بستر مورد نیاز شبکه‌ی TOR.
برنامه با خواندن کلید رجیستری مربوط به هر یک از مرورگران (نام آن‌ها در لیست زیر آمده است) در صورت وجود از نصب آن‌ها در سیستم اطمینان حاصل می‌کند. اطلاعات کلید رجیستری زیر برای نمونه آورده شده است که مربوط به مرورگر Firefox می‌باشد:

HKLM\Software\Clients\StartMenuInternet\Firefox.exe\shell\open\command

مرورگران اینترنتی مورد نظر

- Firefox.exe
- Google Chrome.exe
- Opera.exe
- Safari.exe
- IEXPLORE.EXE

بعد از یافتن یکی از این موارد برای مثال IEXPLORE.EXE پردازه‌ای با دستور CreateProcessInternalW و با پارامتر آمده در شکل زیر آغاز می‌گردد. روش راه اندازی این پردازه به این صورت است که ابتدا پردازه به صورت suspend به وجود می‌آید. در مرحله‌ی بعدی برای تزریق کد از فضای کد و اطلاعات مربوط به خود برنامه‌ی اصلی استفاده شده و کد تزریق شده بر روی اطلاعات اولیه قرار می‌گیرد. بعد از آن با استفاده از دستور ZwSetContentThread نقطه‌ی آغازین برنامه تنظیم شده و پردازه به اجرا در می‌آید.

اطلاعات دیگری که در این بخش از سیستم جمع آوری می شود شامل موارد زیر است:

- Drivers Informaion
- Computer Name
- CPU Information
- IP Address of Victim System

اطلاعات درایور یا درایورهای سیستمی با استفاده از دو متد GetAdapterCount و GetAdapterIdentifier از Interface: Direct3D- Create9 صورت می گیرد.

با جمع آوری این اطلاعات نوبت به ارسال اطلاعات می رسد. بخشی از آدرس سرور خاص این بدافزار به صورت http://ilo**7d**oti**gr. onion است.

همان‌طور که در بالا مشخص است آدرس استفاده شده برای اتصال به سرور مورد نظر بدافزار ساختاری متفاوت از آدرس های معمول دارد. اگر بخواهید در قالب شبکه ی TOR سرویسی به مشترکان ارایه دهید این شبکه به شما قابلیت پنهان سازی سرورتان و در نتیجه مکان فیزیکیتان را می دهد. برای این منظور TOR از فرمت خاصی از آدرس ها بهره می برد که با آدرس های معمول استفاده شده در شبکه ی جهانی متفاوت است. ساختار این آدرس به شکل XYZ.onion است که در آن XYZ تعداد ۱۶ کاراکتر استخراج شده از کلید عمومی سرویس پنهان می باشد.

نکته ی دیگری که در این بخش قابل ذکر است دستورات C&C به کار رفته توسط بدافزار برای بهره گیری از سیستم قربانی در آلوده سازی سیستم های دیگر و یا جمع آوری اطلاعات بیشتر است. در لیست زیر دستورات مربوط را مشاهده می کنید.

C&C instructions

- dlexec: دانلود فایل اجرایی از یک URL و اجرای آن
- dlrunmem: دانلود فایل و تزریق آن در مرورگر
- dltorexec: دانلود فایل اجرایی TOR و اجرای آن
- dltorrunmem: دانلود فایل TOR و تزریق آن در مرورگر
- update: به روز سازی بدافزار
- install: گرفتن فایل جدید و قراردادن آن در مسیر مشخص فایل در Application Data
- installexec: دریافت و اجرای فایل جدید قرار گرفته در Application Data
- kill: پایان دادن به کار

بخش پنجم

کد تزریق شده در مرورگر در واقع اقدام به راه اندازی بستر لازم به کار شبکه ی TOR می کند.

تکنیک های بدافزار

روش نصب، از طریق فایل دانلود کننده و اجرا کننده آن که در مرحله ی اول توضیح داده شده است.

روش بقا از طریق تنظیم شدن کلید run در رجیستری

روش مخفی شدن فایل به این صورت است که فایل های ایجاد شده همگی با مشخصه ی سیستمی و پنهان ایجاد می شوند و برنامه ی اصلی نیز بعد از اجرای اولیه با تزریق در EXPLORER.EXE کار می کند.

روش آنتی دیباگ، در لیست زیر آمده است. تمامی این روش ها برای آگاهی یافتن از وجود دیباگر و در صورت وجود جداسازی برنامه از دسترسی دیباگر است.

- NtSetInformationThread Debugger Detaching
- NtQueryInformationProcess (ProcessDebugObjectHandle)
- NtQueryInformationProcess (ProcessDebugPort)
- NtQueryInformationProcess (ProcessDebugFlags)

روش یا پروتکل ارتباط با شبکه: استفاده از شبکه ی TOR برای برقراری ارتباط. دلیل استفاده از این شبکه سعی در پنهان سازی مقصد نهایی است.

تأیید آسیب پذیری در
آزمون نفوذپذیری
بخش پنجم

در فاز پیشین، آزمون کننده تهدیدات و آسیب پذیری هایی را شناسایی نمود که به مدیران سیستم به منظور بهبود امنیت سیستم هایشان کمک می‌نمود. در این فاز به بررسی آسیب پذیری‌های یافت شده و تأیید هریک از آن‌ها به جهت قابل سوء استفاده بودن و نبودن و این‌که اگر قابل سوء استفاده باشند به چه میزان خطرناک است، پرداخته خواهد شد.

تأیید آسیب پذیری هم‌چون شناسایی آسیب پذیری به دو روش دستی و خودکار صورت می‌گیرد.

مراحل روش دستی به شرح زیر است:

۱- شناسایی برنامه کاربردی اجرا شده
۲- پیدا نمودن اطلاعات مربوط به نسخه برنامه کاربردی
۳- جستجوی اکسپلویت های مربوط به آن در اینترنت
۴- اجرای اکسپلویت ها علیه برنامه کاربردی هدف

این روش سخت و زمان‌بر است به همین دلیل از روش خودکار هم استفاده می‌گردد.

در روش خودکار تأیید آسیب پذیری از ابزارهای غیر رایگانی مانند Nessus و coreimpact استفاده می‌گردد. ابزارهای نام برده شده به منظور ارزیابی آسیب پذیری نیز استفاده می‌گردد. لازم به ذکر است که می توان از ابزارهای رایگان هم استفاده نمود.

به منظور بهره برداری از آسیب پذیری می توان اکسپلویت‌هایی را ایجاد نمود. بدین منظور باید بخش هایی از برنامه کاربردی که قابل بهره برداری می‌باشد تعیین گردد. روش‌های تعیین این مورد به شرح زیر است:

- فازینگ: در این روش داده‌های تصادفی به برنامه فرستاده می‌شود به این امید که آسیب پذیری‌ای شناسایی گردد. حملاتی هم‌چون حمله brute force در دسته حملات fuzzing قرار دارد. ساده ترین استفاده از این حمله را می‌توان به پیدا نمودن نام کاربری و یا رمز عبور دانست.
- بررسی کد: در این روش با بررسی کد برنامه کاربردی می‌توان نقاط آسیب پذیر را پیدا نمود و آن‌ها را به منظور این‌که آیا قابل بهره برداری هستند یا نه آزمایش نمود. از مزایای این روش این است که می‌توان به عملکرد برنامه کاربردی پی برد؛ اما از معایب آن نیز می‌توان به اندازه کدها اشاره نمود. زیرا در صورتی که اندازه کد زیاد باشد استفاده از این روش زمان‌بر است.

در این شماره، به بررسی آسیب‌پذیری‌های یافت شده و اینکه آیا می‌توان از آسیب‌پذیری‌هایی که کشف شده‌اند بهره‌برداری نمود، پرداخته شد. در شماره‌های بعدی به روش‌های به خطر انداختن سیستم و افزایش میزان دسترسی به آن پرداخته خواهد شد.

شمارش معکوس نهایی - آغاز عدم پشتیبانی از ویندوز XP

شرکت مایکروسافت آخرین به‌روز رسانی مربوط به ویندوز xp را در تاریخ ۸ آپریل ۲۰۱۴ عرضه خواهد نمود و پس از آن هیچ به‌روزرسانی و پشتیبانی مربوط به این سیستم عامل وجود نخواهد داشت. بنابراین اگر آسیب پذیری بر روی این سیستم عامل یافت گردید می‌توان از آن برای همیشه سوء استفاده نمود.
این بدان معنا است که مهاجمان می‌توانند با استفاده از خطاهایی که در ویندوز ۷ و۸ وجود دارد و رفع گردیده است، به منظور سوء استفاده از ویندوز XP استفاده نمایند. این امر به این علت است که در تمامی کدهای نسخه های اخیر ویندوز از کدهای ویندوز XP -البته با انجام تغییراتی- استفاده شده است.
اعلان تاریخ به‌روز رسانی، توسط پنجره‌ی popupای که در ویندوز xp نمایش داده می شود، اعلان می‌گردد. البته لازم به ذکر است که اگر ویندوز XP به‌روزرسانی گردد، این پنجره نمایش داده خواهد شد اما در صورتی که ویندوز XP به‌روز رسانی نگردد، این پنجره نمایش داده نخواهد شد.
به‌این منظور شرکت مایکروسافت به کاربران ویندوز XP پیشنهاد نموده است که از نرم افزار Laplink PCMover به منظور انتقال داده‌های خود از ویندوز XP به ویندوز ۷ یا ۸ استفاده نمایند.

مراقب تروجان بانکی Zeus باشید!

یک نوع جدید ازخطرناکترین تروجان بانکی زئوس توسط آزمایشگاه یکی از آنتی ویروس ها، که با گواهی دیجیتال به سرقت رفته شده و متعلق به شرکت مایکروسافت برای جلوگیری از تشخیص از مرورگرهای وب و سیستم های ضد ویروس امضاء گشته بود، شناسایی شده است.
هر کامپیوتری که دارای سیستم عامل ویندوز است این‌گونه تنظیم شده است که نرم افزاری را که با گواهینامه های دیجیتال مایکروسافت "امضا" شده را قبول کند.
مجرمان اینترنتی به نحوی موفق به هک گواهی نامه های دیجیتال معتبر مایکروسافت شده اند، که از آن برای فریب کاربران و مدیران استفاده شده است. از آن‌جا که اجرای آن به صورت دیجیتالی توسط توسعه دهنده مایکروسافت امضاء می‌گردد هیچ آنتی ویروسی نمی تواند آن را پیدا کند.
نرم افزارهای مخرب دیجیتالی امضا شده در سال گذشته توجه بسیاری از رسانه ها را به خود جلب کرده بود. بنا به گزارش‌ها، بیش از ۲۰۰۰۰۰ نرم افزار مخرب منحصر به فرد در دو سال گذشته که با امضای دیجیتال معتبر، امضا شده بود، کشف گردید.
زئوس یکی از قدیمی ترین تروجان های مالی است، اما این نوع از تروجان زئوس توانسته کنترل های امنیتی را به صورت قانونی دور بزند و اقدام به اجرای حملاتی برای به دست آوردن اعتبار لازم به منظور ورود به حساب بانکی قربانیان و ارتکاب تقلب مالی نماید.

سارقان مجازی با نقاب به سمت شما می‌آیند

از ابتدای پدید آمدن شبکه های مخفی با قابلیت پنهان سازی دو سر رابطه انتظار می‌رفت سارقان مجازی از بستر ایجاد شده به نفع خود استفاده کنند. شبکه ی TOR (مخفف The Onion Router) نمونه ای از این شبکه های مخفی است. طراحی این شبکه ها به گونه ایست که توانایی پنهان سازی شناسه ی فرستنده و گیرنده پیام و هم‌چنین محتوای آن را دارا می‌باشند؛ بنابراین در ارسال اطلاعات مثل نقاب عمل می‌کنند. هر پیام برای رسیدن به مقصد خود از سه Relay دیگر در شبکه که به صورت تصادفی انتخاب شده‌اند عبور می‌کند. اطلاعات به همراه مقصد اصلی و Relayهای میانی در مبدأ رمزنگاری می شوند. این رمزنگاری با دریافت کلید عمومی هر یک از Relayهای میانی صورت می‌گیرد. لایه های رمزنگاری به گونه ای قرار دارند که در هر مرحله تنها آدرس Relay بعدی و قبلی مشخص است. در آخرین Relay، آخرین رمزگشایی صورت گرفته و متن اصلی به مقصد نهایی ارسال می‌شود. دلیل نام گذاری این شبکه هم به نام شبکه ی پیازی، به دلیل استفاده از لایه های چندگانه ی رمزنگاری است که هر لایه در یک مرحله رمزگشایی شده تا دستیابی به لایه ی بعدی امکان پذیر باشد. برای کسب اطلاعات بیشتر به آدرس زیر مراجعه کنید.
https://www.torproject.org/about/overview.html.en
همزمان با افزایش استفاده از شبکه های مخفی ساز شاهد بالا رفتن آمار بدافزارهای پیاده سازی شده در این بستر نیز هستیم. بدافزار Atrax که با نام Win32.AtraxBot.a Spy شناسایی می شود نمونه ای از سارقان مجازی است که در اواسط سال ۲۰۱۳ میلادی شناسایی شد. به طور کلی می‌توان گفت طراحی این بدافزار در ابتدا به منظور جمع آوری اطلاعات از سیستم قربانی و ارسال آن به سرورهای مورد نظرش در بستر شبکه ی TOR بوده است. بعد از محقق شدن این کار، بدافزار اقدام به برقراری ارتباطات c&c برای دریافت اطلاعات و دستورات جدید هم خواهد کرد.

عبور از خان هشتم؛ کشف یک روت‌کیت جدید توسط کارشناسان امن‌پرداز

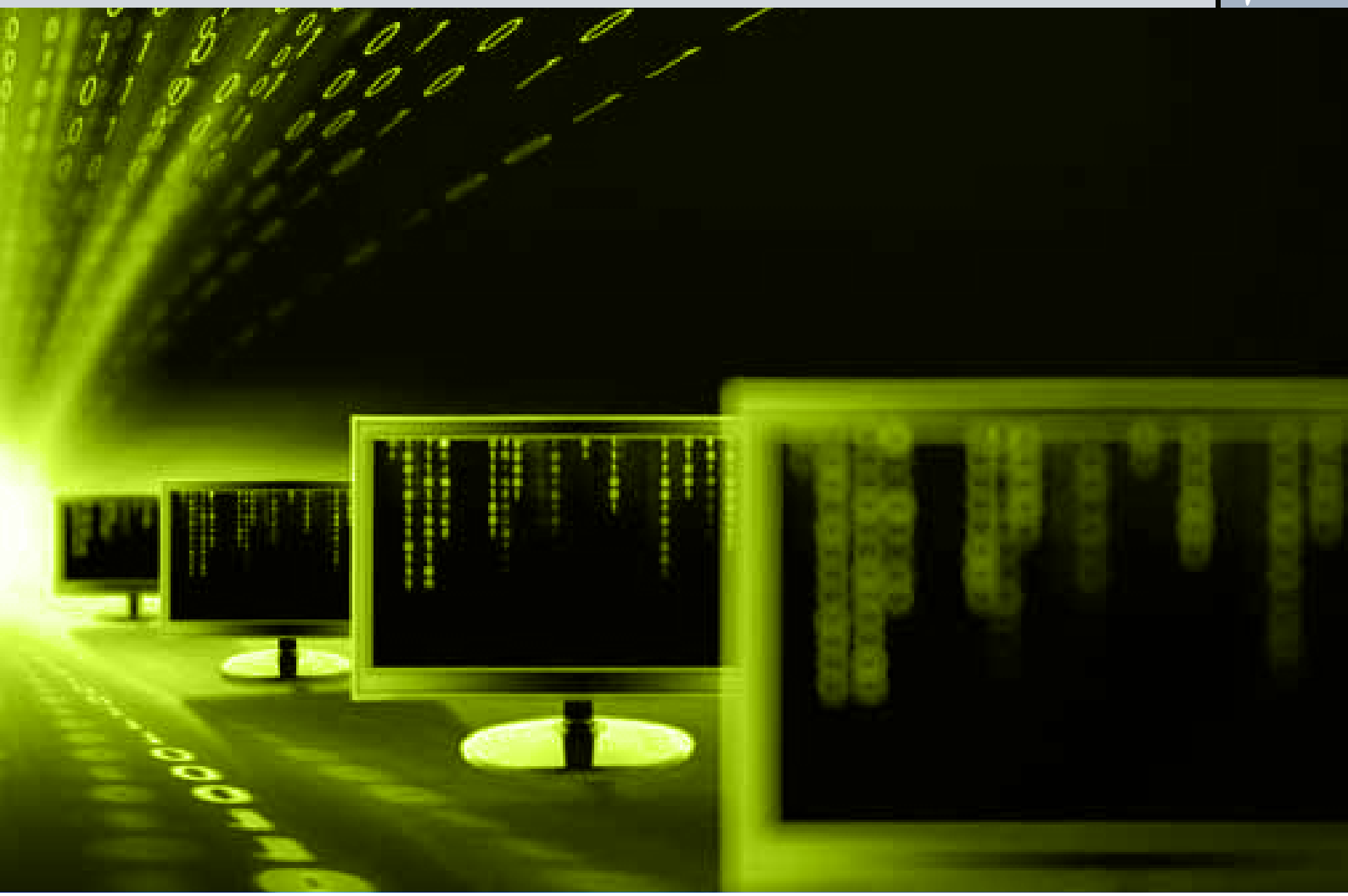
آزمایشگاه تحلیل بدافزار پادویش از کشف یک بدافزار جدید با قابلیت ارسال هرزنامه خبر داد. این بدافزار که هم‌چنان توسط ضدویروس‌ها شناسایی نمی‌شود، علاوه بر آلوده‌سازی و پنهان شدن در نسخه‌های مختلف ویندوز، قابلیت آلوده‌سازی آخرین نسخه ویندوز مایکروسافت (نسخه ۸.۱) را نیز داراست.
به گزارش تیم تحلیل شرکت نرم‌افزاری امن‌پرداز، این بدافزار که Rootkit.win32.Damon.A نامیده شده است، از نوع روت‌کیت همراه با قابلیت‌های بوت‌کیت بوده و خود را در سیستم کاربر مخفی می‌کند. سپس با اتصال به سرور فرماندهی و کنترل خود، از سیستم کاربر برای ارسال هرزنامه سوءاستفاده می‌کند.
داشتن امکان آلوده‌سازی آخرین نسخه‌های ویندوز، آلوده‌سازی نسخه ۶۴ بیتی ویندوز، پنهان شدن از چشم کاربر، اجرا از طریق بوت‌کیت و کنترل از راه دور آن توسط سازندگان این ویروس، آن را بسیار خطرناک نموده است.

آلوده شدن ۱ نفر از ۳۰ نفر به تروجان CryptoLocker!

تحقیقات اخیر دانشگاه Kent بر روی جمعی از جوانان نشان داد که سیستم‌های ۱ نفر از ۳۰ نفر از این جامعه آزمایشی، به تروجان CryptoLocker آلوده می‌گردد که تنها ۱ نفر از ۱۰ نفر آن‌ها این آلودگی را گزارش می‌دهد.
نتایج حاصل از این تحقیقات نشان دهنده این است که تنها یک سوم از این افراد از فایروال استفاده می‌نمایند. که به منظور افزایش این میزان لازم است که اعلان و آگاهی عمومی در مورد خطرات بدافزارها و تهدیدات برخط برای همه‌ی افراد جامعه صورت گیرد.

'عصب بینایی' - هک تصاویر شخصی وب کم میلیون‌ها کاربر یاهو توسط NSA

NSA با کمک یکی از همکاران انگلیسی خود توانست تصویر وب کم کاربران یاهو را در سال‌های ۲۰۰۸ تا ۲۰۱۰ ضبط و ذخیره نماید. این امر هر ۵ دقیقه و به صورت انتخابی تصادفی از کاربران ویدئو چت یاهو صورت گرفته است. لازم به ذکر است که این پروژه با هدف کاربر خاصی صورت نگرفته است. البته شرکت یاهو هرگونه اطلاع قبلی در مورد این برنامه را انکار نمود و اعلام نمود که هیچ گونه همکاری و مشارکتی در اجرای این برنامه با دولت نداشته است.
با توجه به این اقدام، می‌توان نتیجه گرفت که حریم شخصی افراد توسط دولتی که مردم به آن اطمینان دارند به راحتی و به صورت غیرقانونی از بین رفته است.



مدیریت امنیت اطلاعات

بخش پنجم

در شماره‌های پیشین به بررسی و معرفی فازهای پیاده سازی سیستم مدیریت امنیت اطلاعات پرداخته شده بود. در این شماره و در مقاله پیش رو به بررسی آخرین فاز در پیاده سازی سیستم مدیریت امنیت اطلاعات و خلاصه‌ای از آن پرداخته شده است.

فاز اقدام

در این فاز براساس نتایج حاصل شده از فاز بررسی، به منظور تصحیح موارد ترمیمی و بازنگری در نحوه مدیریت اطلاعات پرداخته می‌شود. که شامل موارد زیر است:

۱. پیاده سازی بهبودهای شناسایی شده

در فاز بررسی به نظارت و بازنگری اثرات سیستم مدیریت امنیت اطلاعات پرداخته شد و خروجی این فاز شامل پیشنهادهایی به منظور بهبود آن است؛ در فاز اقدام، پیشنهادهای ارائه شده در فاز پیشین پیاده سازی می‌گردد که این پیشنهادها ممکن است حاصل از بازنگری فعالیت‌های سیستم مدیریت امنیت اطلاعات و ممیزی داخلی باشد. لازم به ذکر است که به منظور اجرای این فاز نیاز به موافقت مدیریت می‌باشد.

۲. ارتباط و انتقال نتایج: توسعه سازمانی

اصلاحات جدید که در اثر پیاده سازی سیستم مدیریت امنیت اطلاعات ایجاد گشته است، نیازمند توسعه بخش هایی است که تغییرات بر روی آن‌ها تأثیر گذاشته است. این نیاز ممکن است در آگاهی، آموزش، آگاهی تمامی کارمندان، و آموزش پرسنل فنی باشد.

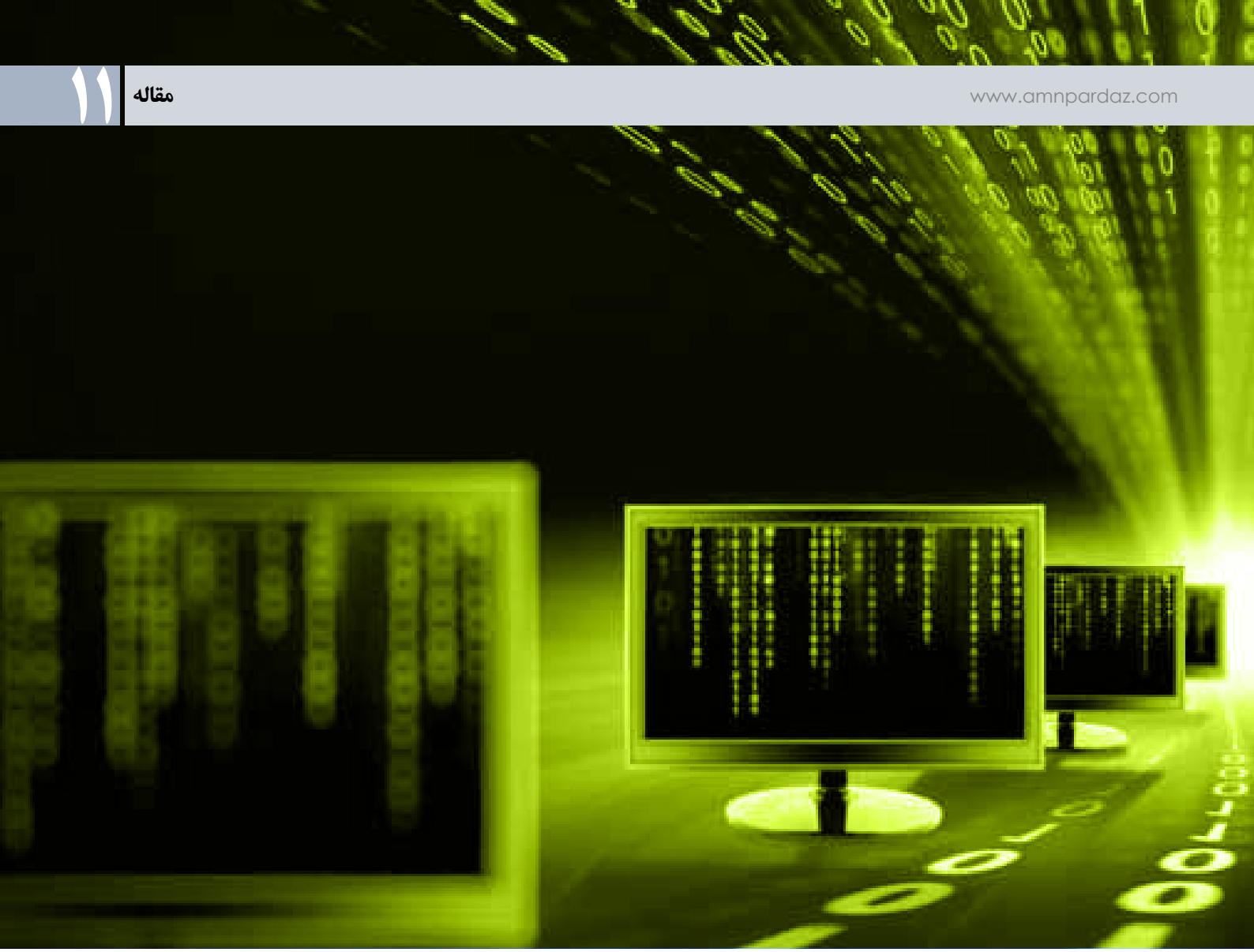
۳. اطمینان از هدف

پس از پیاده سازی کنترل های امنیتی، نیاز به بررسی و تأیید کنترل های اعمال شده با هدف اطمینان از این‌که کنترل پیاده سازی شده است و اثربخش بوده است، وجود دارد. این تأیید و اعتبار سنجی جهت حصول اطمینان از این می باشد که کنترل های امنیتی با اهداف سیستم مدیریت امنیت اطلاعات سازگار است و آن‌ها را پوشانده است.

۴. ادامه روند

امنیت یک فرآیند است نه یک مقصد. اتمام فاز اقدام، منجر به تکرار فاز برنامه ریزی با تمرکز بر اثرات آسیب پذیری های جدید، تغییر محیط فنی و تغییر محیط کسب و کار می‌شود.

اجرای ارزیابی ریسک مجدد نباید بیش از ۱۲ ماه از ارزیابی پیشین



صورت گیرد.

۵. خلاصه مستندات فاز اقدام

درفاز اقدام، با توجه به جزئیات به‌دست آمده از فاز بررسی، سیستم مدیریت امنیت اطلاعات اصلاح می‌گردد. سازمان‌ها ممکن است تمایل به دریافت جزئیات فاز اقدام به منظور انتشار آن در سراسر سازمان داشته باشد. مدارک حاصل از فاز اقدام شامل موارد زیر است:

- راهنمای فاز اقدام
- معیارهای اندازه گیری
- به روز رسانی احتمال خطرات
- چک لیست ممیزی
- نتایج حاصل از ممیزی داخلی
- لیست اقداماتی جهت بهبود سیستم مدیریت امنیت اطلاعات

خلاصه‌ای از پیاده سازی ISMS

هدف از انجام فازهای برنامه ریزی- اجرا- بررسی و اقدام، پیاده سازی سیستم مدیریت امنیت اطلاعات است. هر یک از فازهای بیان شده جنبه‌های متفاوتی از استقرار، پیاده سازی، مدیریت و نگهداری سیستم مدیریت امنیت اطلاعات را پوشش می‌دهد. در طول اجرای فازهای فوق، مستندات زیر تهیه و تدوین می‌گردد:

- سیاست های سیستم مدیریت امنیت اطلاعات
- دامنه سیستم مدیریت امنیت اطلاعات
- تهیه لیستی از عملکردهای مهم کسب و کار
- تشخیص عملیات مهم و کلیدی کسب و کار
- تهیه لیستی از دارایی‌های اطلاعاتی و فن آوری اطلاعاتی مهم با طبقه بندی در زمینه پشتیبانی از عملکرد کسب و کار

- سیاست های امنیتی سیستم مدیریت امنیت اطلاعات
- سیاست های حاکم بر انتخاب و پیاده سازی کنترل های امنیتی، به عنوان مثال، سیاست رمز عبور
- رویه های سیستم مدیریت امنیت اطلاعات
- چگونگی پیاده سازی سیاست ها
- استانداردهای سیستم مدیریت امنیت اطلاعات
- کنترل های خاص به منظور پیاده سازی سیاست ها
- متدولوژی ارزیابی ریسک
- مستنداتی در رابطه با اینکه سازمان چگونه ارزیابی ریسک را انجام می‌دهد.
- یافته های حاصل از ارزیابی ریسک
- محصولات حاصل از ارزیابی ریسک در زمانی که در سازمان اعمال می‌شود.
- پیاده سازی چرخه PDCA
- برنامه مقابله با خطر
- روش ها
- یادداشت ها

شرکت نرم افزاری

امن پرداز

آدرس: تهران، خیابان ملاصدرا، خیابان شیخ بهایی جنوبی، گرمسار غربی، پلاک ۷۶
تلفن: ۰۲۱-۴۳۹۱۲۰۰۰ فکس: ۰۲۱-۴۳۹۱۲۸۰۰
www.amnpardaz.com
info@amnpardaz.com