خبرنامه مرکز تخصصی آپای دانشگاه ایلام

شماره اول - مهر ماه ۱۳۹۶

برگزار شد

برگزاری کارگاه بررسی تهدیدات امنیتی در لایه کاربرد شبکه

برگزاری کارگاه آشنایی با تهدیدات امنیتی در اندروید

- جدیدترین اخبار مربوط به حوزه امنیت
- معرفی جدیدترین بد افزارها
- هشدارها و راهنمایی های امنیتی
- اخبار مرکز تخصصی آپای دانشگاه

فهرست

هشدار: درب پشتی بر روی محصولات NetSarang

هکرها هر روزه در حال پیشرفت هستند و از روشهای جدیدی برای گرفتن قربانیان خود استفاده می کنند. حملات هکری تنها برای نفوذ به سیستم های شخصی و یا گوشی های تلفن همراه هوشمند نیست. بسیاری از این گونه حملات برای دراختیار گرفتن شبکه های بزرگ که دارای اطلاعات مهم بر روی سرورهای خود هستند می باشد. جهت انجام این گونه حملات نفوذگران روشهای مخفی و جالبی را برای موفقیت خود در نفوذ ابداع می کنند.

بر اساس گزارشی که به تازگی توسط محققان امنیت سایبری کمپانی KasperSky منتشر شده است، یک درب پشتی (Backdoor) مخفی بر روی یکی از محصولات مهم شبکه قرار داده شده است. این درب پشتی که با کد نام ShadowPad معرفی شده است بر روی نرم افزار به روز رسانی شده برخی محصولات کمپانی NetSarang کشف شده است که این محصول در کشور ما هم بسیار مورد استفاده قرار می گیرد. توسط این درب پشتی، نفوذگر می توان کنترل کامل بر روی شبکه مخفی پشت این محصولات را در کنترل بگیرد که محصولات این کمپانی، در شبکه های بانکی، شبکه شرکت های داروسازی و پزشکی، ارائه دهندگان خدمات مخابراتی، شرکت های هواپیمایی و غیره... مورد استفاده قرار می گیرند.

بر اساس گزارش منتشر شده توسط کاسپراسکی، نفوذگران با دزدیدن مکانیزم به روز رسانی نرم افزارهای این کمپانی، درب پشتی کاملا مخفیانه و حرفه ای را بر روی سیستم software update قرار داده و به صورت خودکار، همراه با مجوز کامل و گواهی قانونی امضا شده (legitimate signed certificate) کد مخرب درب پشتی را بر روی سیستم های قربانی ارسال و نصب می کردند. این Backdoor مخفی در کتابخانه dll.nssock۲ بر روی نرم افزارهای Xmanager و Xshell قرار داده شده است.

در تاریخ ۴ جولای کمپانی کاسپراسکی این درب پشتی را بر روی محصولات فوق به کمپانی NetSarang گزارش می دهد که این کمپانی سریعا مشکل را بررسی کرده و رفع نموده است. محصولاتی که این حمله بر روی آنها صورت گرفته است عبارتند از:

- Xmanager Enterprise ۵/۰ Build ۱۲۳۲
- Xmanager ۵/۰ Build ۱۰۴۵
- Xshell ۵/۰ Build ۱۳۲۲
- Xftp ۵/۰ Build ۱۲۱۸
- Xlpd ۵/۰ Build ۱۲۲۰

این حمله، یادآور حمله ای مشابه توسط سازندگان باج افزار Petya/NotPetya در تیرماه امسال می باشد که توسط تغییراتی که در سیستم به روز رسانی نرم افزاری خاص سیستم امور مالیاتی کشور اوکراین داده شده در سطح وسیعی از ساختارهای مالیاتی آن کشور انتشار یافته است. هکرها این درب پشتی را توسط چندین لایه رمزنگاری آماده سازی و بر روی سیستم به روز رسانی قرار داده اند که تنها در برخی موارد خاص، رمزگشایی آن صورت می گرفته است. این کار برای بهتر کردن عملکرد درب پشتی جهت مخفی ماندن آن می باشد. تا هنگامی که packet های خاصی که حاوی دستورالعمل های اجرایی می باشدن از جانب سرور C&C برای درب پشتی ارسال نشود، این backdoor فعالیت خاصی را از خود نشان نمی دهد تا همچنان مخفی بماند.

هشدار: درب پشتی بر روی محصولات NetSarang (...)

پس از آن، درب پشتی هر ۸ ساعت یکبار اقدام به ارسال برخی اطلاعات سیستم قربانی برای سرور خود می کند.
فعال سازی این درب پشتی پس از نصب بر روی سیستم قربانی، توسط یک پیغام DNS TXT Record صورت می گیرد که از یک دامنه خاص برای آن ارسال می گردد که این دامنه در طول ماه گذشته register شده و عملیات DNS lookup بر روی آن انجام می گردد. پس از نصب درب پشتی بر روی سیستم قربانی و معرفی خود به سرور C&C، از طرف سرور کلید رمزگشایی برای انجام قدم های بعدی عملکرد درب پشتی ارسال می شود و درب پشتی را فعال می کند. پس از فعال سازی، این درب پشتی امکان اجرای دستورات از راه دور و همچنین اجرای پروسه های جدید را برای هکر بر روی سیستم قربانی از راه دور فراهم می آورد.
اگر از این محصولات در ساختار شبکه خود استفاده می کنید، جهت مشخص شدن این موضوع که آیا این درب پشتی بر روی سیستم های شما وجود دارد یا خیر، می توانید با چک کردن رکوردهای DNS به دامنه های زیر در داخل شبکه خود، وجود یا عدم وجود درب پشتی را مشخص کنید. در صورت وجود این گونه رکوردها، درخواست ها به دامنه های زیر را حتما در شبکه خود block نمایید:

- ribotqtonut[.]com
- nylalobghyhirgh[.]com
- jkvmdmjyfcvkf[.]com
- bafyvoruzgjitwr[.]com
- xmponmzmxkxkh[.]com
- tczafklirkl[.]com
- notped[.]com
- dnsgogle[.]com
- operatingbox[.]com
- paniesx[.]com
- techniciantext[.]com

به یاد داشته باشید که حتما نرم افزارهای آسیب پذیر که در بالا اشاره شد را به روز رسانی کنید، چراکه نسخه به روز شده که این مشکل در آن رفع شده است بر روی وب سایت سازنده جهت دانلود قرار داده شده است.

کشف باگ جدید در پروتکل NTLM ویندوز

این ماه مایکروسافت یک وصله ی امنیتی، برای یک آسیب پذیری جدی (ارتقاء دسترسی) منتشر نموده است که تمامی نسخه های ویندوز، از ۲۰۰۷ به بعد را تحت تأثیر قرار می دهد.

محققان امنیتی شرکت Preemptدو آسیب‌پذیری zero-day در پروتکل امنیتی NTLMویندوز کشف کرده اند، هر دوی این آسیب پذیری‌ها به مهاجم اجازه می دهند که یک دامنه جدید ایجاد نموده و آن را به طور کامل کنترل نماید.

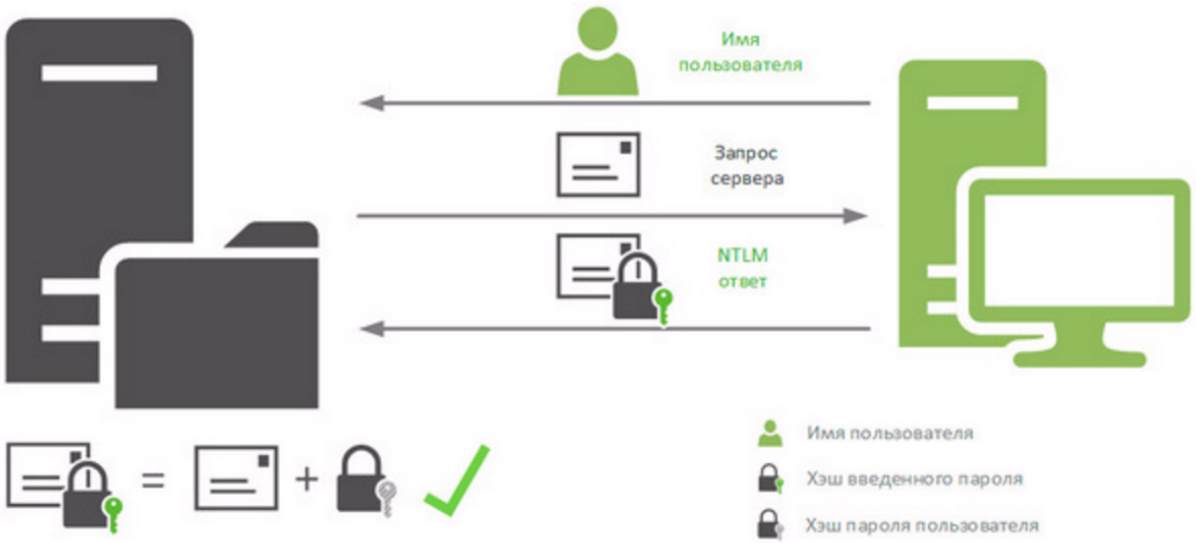
NTLM (NT LAN Manager) یک پروتکل احراز هویت قدیمی است که در شبکه های شامل سیستم عامل های ویندوز و همچنین در سیستم های مستقل مورد استفاده قرار می‌گیرد.

اگرچه NTLMتوسط Kerberosدر ویندوز ۲۰۰۰جایگزین شده است که امنیت بیشتری را در سیستم های شبکه ای فراهم آورد، اما همچنان توسط مایکروسافت پشتیبانی می‌شود و کماکان به صورت گسترده مورد استفاده قرار می‌گیرد.

در NTLM، به سادگی، هر زمان که یک کاربر می‌خواهد به سرور متصل شود، سرور یک challengeرا مطرح می‌کند و کاربر challengeرا با پسورد هش خود رمزگذاری می‌کند. مهاجم می‌تواند یک نشست همزمان با سروری که می‌خواهد به آن حمله کند ایجاد نماید و از همان Challengeاستفاده کند، و همان هش رمزگذاری شده را به منظور ایجاد یک احراز هویت موفق در NTLMارسال نماید. با استفاده از احراز هویتِ موفقیت‌آمیزِ NTLM، مهاجم می‌تواند یک نشست SMB(Server Message Block) را باز نموده و سیستم هدف را با نرم‌افزارهای مخرب آلوده کند.

اولین آسیب پذیری، Lightweight Directory Access Protocol(LDAP) حفاظت نشده از NTLMرا درگیر می‌کند، و دومی Remote Desktop Protocol (RDP) را تحت تأثیر قرار می دهد.

LDAPبه اندازه کافی در مقابل حملات NTLMمقاوم نیست، حتی زمانی که LDAPساخته شده و معیارهای دفاعی



کشف باگ جدید در پروتکل NTLM ویندوز (...)

برای آن مشخص گردیده است تنها از حملات Man-in-the-middle(MitM)محافظت می‌کند، نه از رد و بدل شدن اعتبارسنجی ها.

این آسیب‌پذیری به مهاجم با دسترسی SYSTEMبر روی سیستم هدف، اجازه می‌دهد که از نشست های NTLM ورودی استفاده نموده و عملیات LDAPرا انجام دهد، مانند به روزرسانی objectهای دامنه از طرف کاربر NTLM.

Yaron Zinarاز Preemptدر رابطه با جزئیات آسیب‌پذیری می‌گوید: "به منظور پی بردن به میزان حساسیت موضوع، باید تمامی پروتکل های ویندوز، که از APIاحرازِ هویتِ ویندوز (SSPI) استفاده می‌کنند و اجازه می دهند نشست احراز هویت به سمت NTLMسوق یابد را بررسی نمود."

" درنتیجه، هر اتصالی در سیستم‌های مورد استفاده نظیر (SMB, WMI, SQL, HTTP) با کاربری ادمین به مهاجم اجازه دسترسی به تمام قابلیت‌های ویندوز را می‌دهد. "

دومین آسیب‌پذیریِ NTLMپروتکل Remote Desktop Protocol Restricted-Admin mode را تحت تأثیر قرار می‌دهد. حالتِ RDP Restricted-Admin به کاربران این امکان را می‌دهد که بدون وارد نمودن پسورد از راه دور به یک کامپیوتر متصل گردند.

به گفته‌ی محققانِ Preempt، RDP Restricted-Adminبه سیستم‌های احراز هویت اجازه می‌دهد که به سمت NTLM سوق یابند. این بدان معنی است که حملات صورت گرفته با NTLM،مانند اعتبارسنجی و کرک نمودن پسورد، علیه RDP Restricted-Adminنیز می‌تواند اجرا گردد.

زمانی که با آسیب‌پذیری LDAPهمراه باشد، مهاجم می‌تواند هر زمان که یک ادمین با RDP Restricted-Admin متصل می‌شود یک دامنه ی جعلی با حساب کاربری ادمین ایجاد نماید و کنترل کل دامنه را به دست بگیرد.

محققان در ماه آپریل آسیب‌پذیری‌های LDAPو RDPدر NTLMرا کشف نموده و به صورت مخفیانه به مایکروسافت گزارش نمودند. با این حال، مایکروسافت آسیب‌پذیری NTLM LDAPرا در ماه مَی اعلام کرد، و نام CVE-۲۰۱۷-۸۵۶۳را به آن اختصاص داد، اما باگ RDPرا رد نمود، و ادعا کرد که این یک مسئله ی شناخته شده است و باید جهت مصون ماندن از هر گونه حمله ی NTLMشبکه را پیکربندی نمود.

مایکروسافت در مشاوره خود توضیح داد: "در سناریوی یک حمله ی از راه دور، مهاجم می‌تواند با اجرای یک اپلیکیشن خاص جهت ارسال ترافیک مخرب به Domain Controller این آسیب پذیری را اکسپلویت نماید. مهاجمی که موفق به اکسپلویت نمودن این آسیب پذیری شد می‌تواند پروسه ها را در یک بستر بالقوه اجرا کند."

برگزاری نشست آشنایی با امنیت در حوزه فناوری اطلاعات

با دعوت مرکز آپا، روز شنبه مورخ ۵ اردیبهشت نشستی جهت معرفی خدمات مرکز آپا و ارتباط نزدیکتر با مراکز فناوری اطلاعات سازمان ها و ادارات دولتی استان برگزار گردید.

میهمانان ویژه این جلسه جناب سرهنگ جمالی رئیس پلیس فضای تولید و تبادل اطلاعات استان ایلام، جناب آقای مهندس حسن بیگی رئیس شرکت ارتباطات زیر ساخت و جناب آقای مهندس بیرامی مدیر کل ارتباطات و فناوری اطلاعات استان ایلام بودند و مهمانان و مخاطبان این دوره مدیران و کارشناسان فناوری اطلاعات سازمان ها و ادارات دولتی و برخی شرکتهای خصوصی استان ایلام بودند.

در آغاز این نشست دکتر مهدی زاده به معرفی مرکز آپا و خدمات قابل ارائه در این مرکز پرداخت و گزارشی از فعالیت های این مرکز در سال ۱۳۹۵ ارائه نمود.

در ادامه مهندس بیرامی ضمن تشکر از خدمات مرکز آپا و تلاش معاونت پژوهش و فناوری دانشگاه در راستای توانمندسازی این مرکز، به بیان ضرورت استفاده از خدمات مرکز آپا پرداخت.

سخنران سوم این نشست سرهنگ جمالی بود که با ابراز خرسندی از فعال شدن مرکز آپای ایلام و تشکر از برگزاری این نشست به معرفی خدمات پلیس فتا پرداخت.

در ادامه این نشست دو کارگاه آموزشی در خصوص امنیت برگزار شد و در فاصله برگزاری دو کارگاه و در قالب بحث آزاد شرکت کنندگان به تبادل نظرات و تجربیات خود اقدام نمودند.

برگزاری کارگاه آشنایی با تهدیدات امنیتی در اندروید

در نخستین کارگاه "نشست آشنایی با امنیت در حوزه فناوری اطلاعات"، جناب آقای دکتر بگ‌محمدی عضو هیات علمی مرکز آپای ایلام کارگاهی با عنوان "آشنایی با تهدیدات امنیتی در اندروید" برگزار نمونند.

دکتر بگ‌محمدی در این کارگاه ضمن بررسی میزان محبوبت اندروید در بین سیستم عامل های موبایل و ارائه آماری از میزان استفاده گوشی های اندرویدی در ایران؛ به اهمیت موضوع امنیت در سیستم عامل اندروید پرداخت.

در بخش های مختلف این کارگاه ضمن ارائه مثالهای کاربردی در زمینه ضعف امنیتی نرم افزارهای طراحی شده برای این سیستم عامل و زمینه های بروز مشکلات امنیتی در اندروید پرداخته شد. در ادامه ضمن بررسی معماری این سیستم عامل و روش طراحی نرم افزارهای اندروید به معرفی روشهایی جهت بررسی امنیتی نرم افزارها و ارتباطات شبکه ای این سیستم عامل پرداخته شد.

در بخش مهمی از این کارگاه ضمن معرفی چند ابزار کاربردی جهت بررسی امنیت نرم افزارهای طراحی شده برای اندروید به بررسی علل ضعف های آن و رخنه های ایجاد شده توسط این ضعف ها پرداخته شد.

در بخش پایانی این کارگاه و در قالب پرسش و پاسخ به سوالات حاضران در خصوص تهدیدات امنیتی در اندروید پرداخته شد.

برگزاری کارگاه آشنایی با تهدیدات لایه کاربرد

دکتر محمد تنهایی، عضو هیات علمی مرکز آپای ایلام در دومین کارگاه از "نشست آشنایی با امنیت در حوزه فناوری اطلاعات" به بررسی تهدیدات امنیتی در لایه کاربرد شبکه پرداخت و ضمن تبیین موضوع اهمیت امنیت در شبکه، با ذکر مثال چندین مورد را بررسی نمود.

در بخشی از این کارگاه دکتر تنهایی با بیان این موضوع که ۷۵٪ حملات فضای وب در لایه کاربرد روی می دهد به ضرورت موضوع آشنایی با این حملات و روشهای جلوگیری از آنها پرداخت.
در ادامه و با بررسی ۶ نوع از حملات پرکاربرد در این حیطه و آشنایی با مکانیزم هر کدام از حملات؛ مطالبی را در مورد شیوه های مقابله با این تهدیدات بیان نمودند. بررسی حملات DOS و DDOS و اهمیت استفاده از CDN بومی برای مقابله با اینگونه حملات بخش دیگری از این کارگاه بود.

در بخش پایانی این کارگاه که به صورت پرسش و پاسخ برگزار گردید، شرکت کنندگان با بیان نظر خود در خصوص روشهای کاربردی و یا ابداعی مقابله با حملات فرض شده اهمیت موضوع امنیت در لایه کاربرد را مورد بررسی قرار دادند.

مرکز تخصصی آپای دانشگاه ایلام

پست الکترونیکی cert@ilam.ac.ir

وب سایت cert.ilam.ac.ir