ЗАЩИТА БЕЗ ИЛЛЮЗИЙ

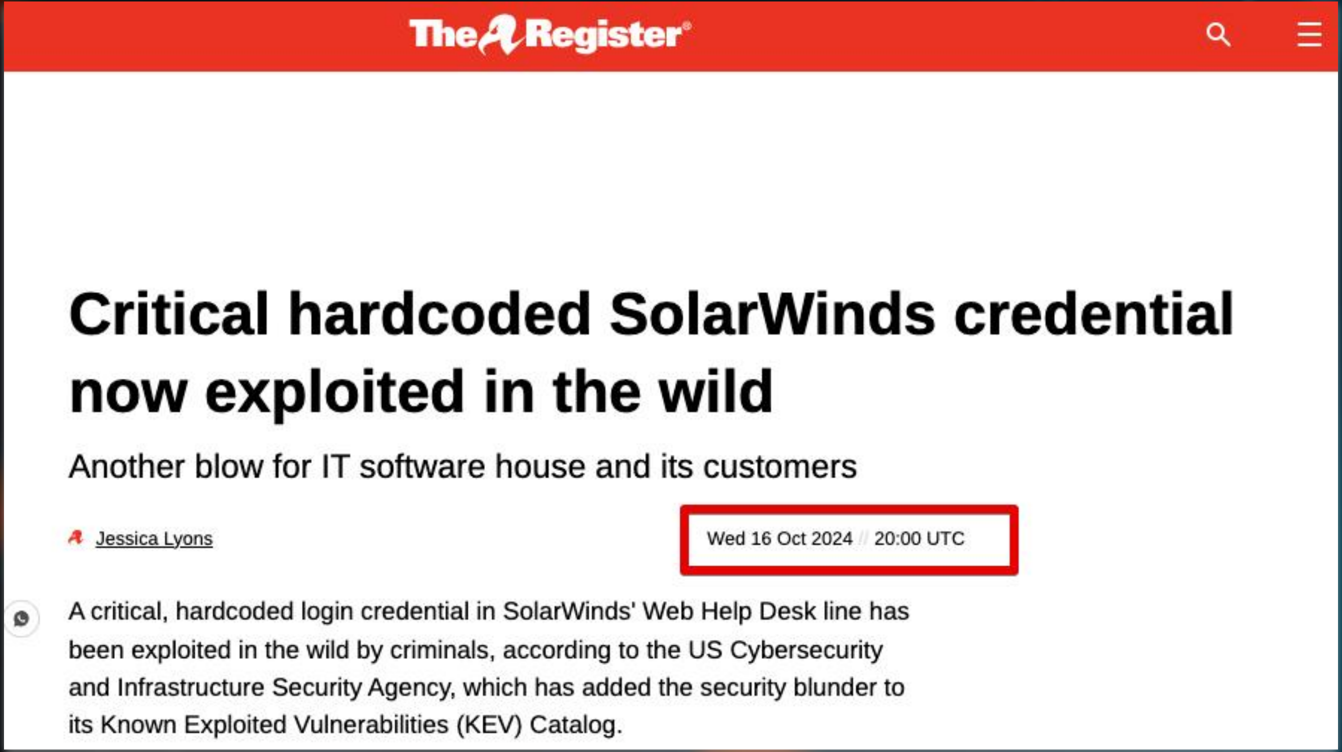
Yevgeniy Goncharov, 2024

Кто сказал, что так надо?

- “Эти” продукты использовать
- “Эти” продукты использовать “там” и “там”
- “Эти” продукты использовать “так-то” и “так-то”
    - “Эти” продукты используем “100 лет” (историзм)
    - “Эти” продукты безопасны
        - Откуда взялось это принятие на веру, кто его привил?
        - Соответствие стандартам скажете Вы. Вот - критерий выбора продукта!

Не хардкодить пароли

fail



The Register®

Critical hardcoded SolarWinds credential now exploited in the wild

Another blow for IT software house and its customers

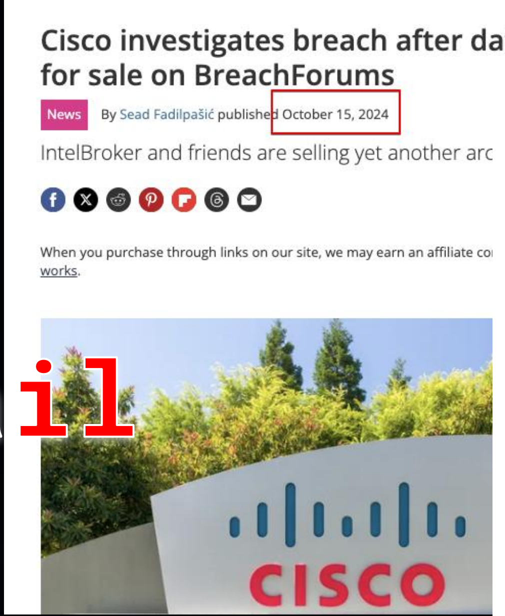
Jessica Lyons

Wed 16 Oct 2024 // 20:00 UTC

A critical, hardcoded login credential in SolarWinds' Web Help Desk line has been exploited in the wild by criminals, according to the US Cybersecurity and Infrastructure Security Agency, which has added the security blunder to its Known Exploited Vulnerabilities (KEV) Catalog.

https://www.theregister.com/2024/10/16/solarwinds_critical_hardcoded_credential_bug/

Хранить данные в конфиденциальности



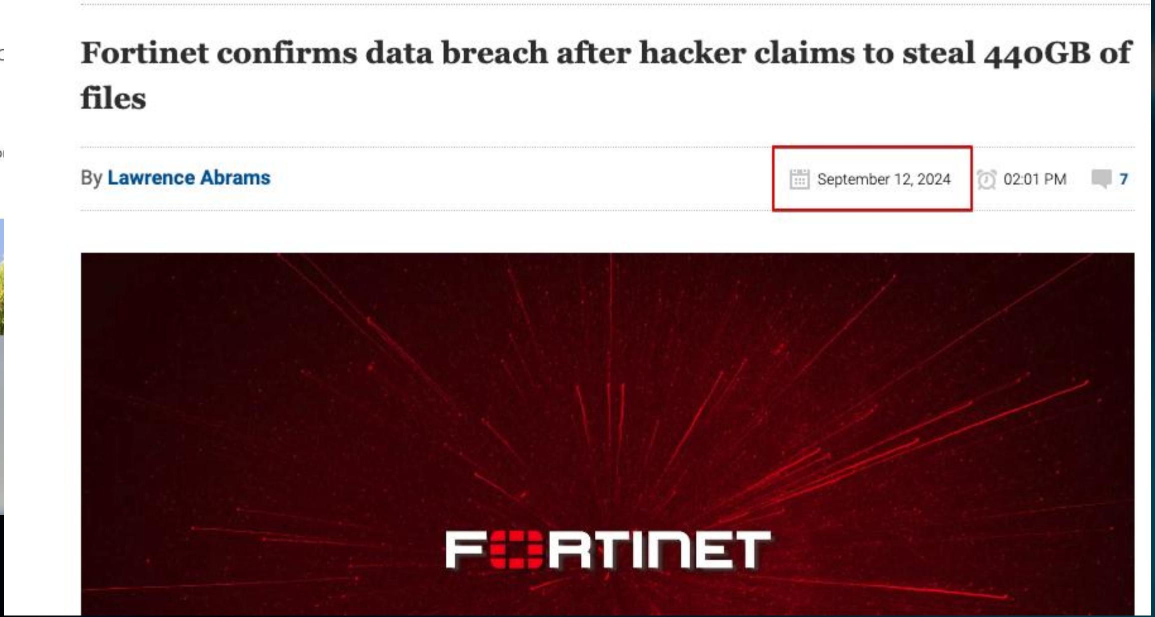
Cisco investigates breach after data put up for sale on BreachForums

News By Sead Fadilpašić published October 15, 2024

IntelBroker and friends are selling yet another arc

When you purchase through links on our site, we may earn an affiliate co works.

fail



Fortinet confirms data breach after hacker claims to steal 440GB of files

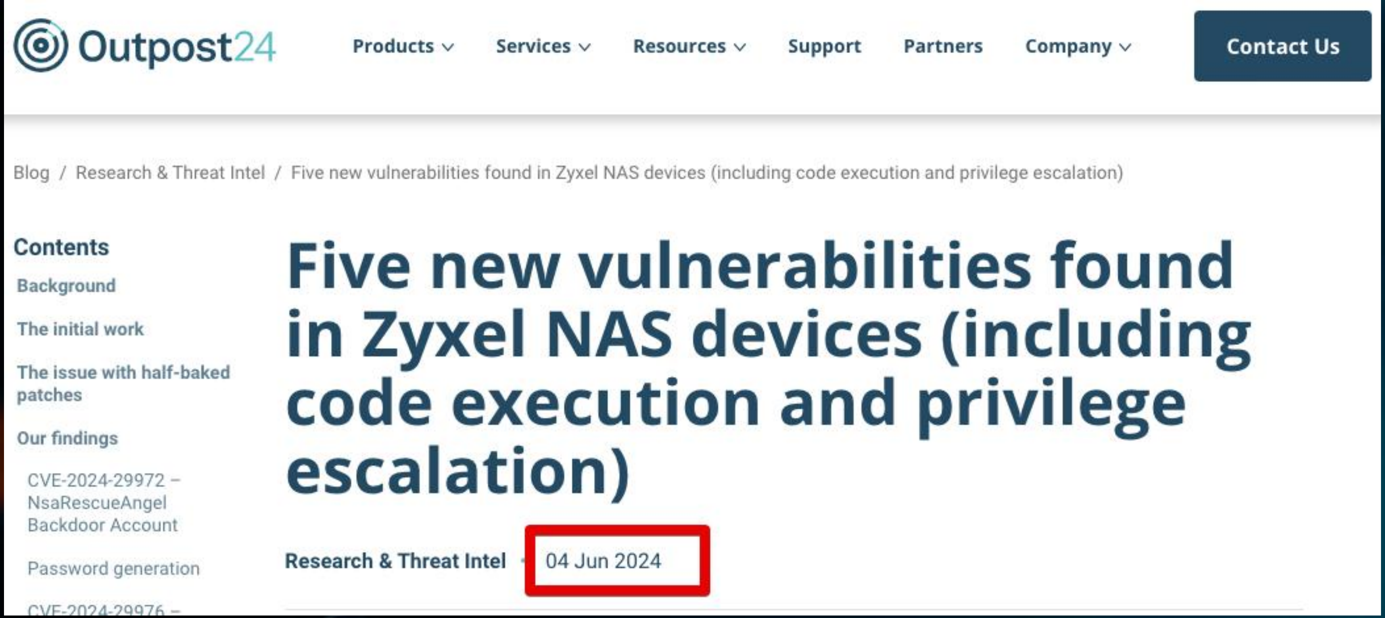
By Lawrence Abrams September 12, 2024 02:01 PM 7

https://www.techradar.com/pro/security/cisco-investigates-breach-after-data-put-up-for-sale-on-breachforums

https://www.bleepingcomputer.com/news/security/fortinet-confirms-data-breach-after-hacker-claims-to-steal-440gb-of-files/

Хранить данные на защищенных носителях

fail



Blog / Research & Threat Intel / Five new vulnerabilities found in Zyxel NAS devices (including code execution and privilege escalation)

Contents

Background

The initial work

The issue with half-baked patches

Our findings

CVE-2024-29972 – NsaRescueAngel Backdoor Account

Password generation

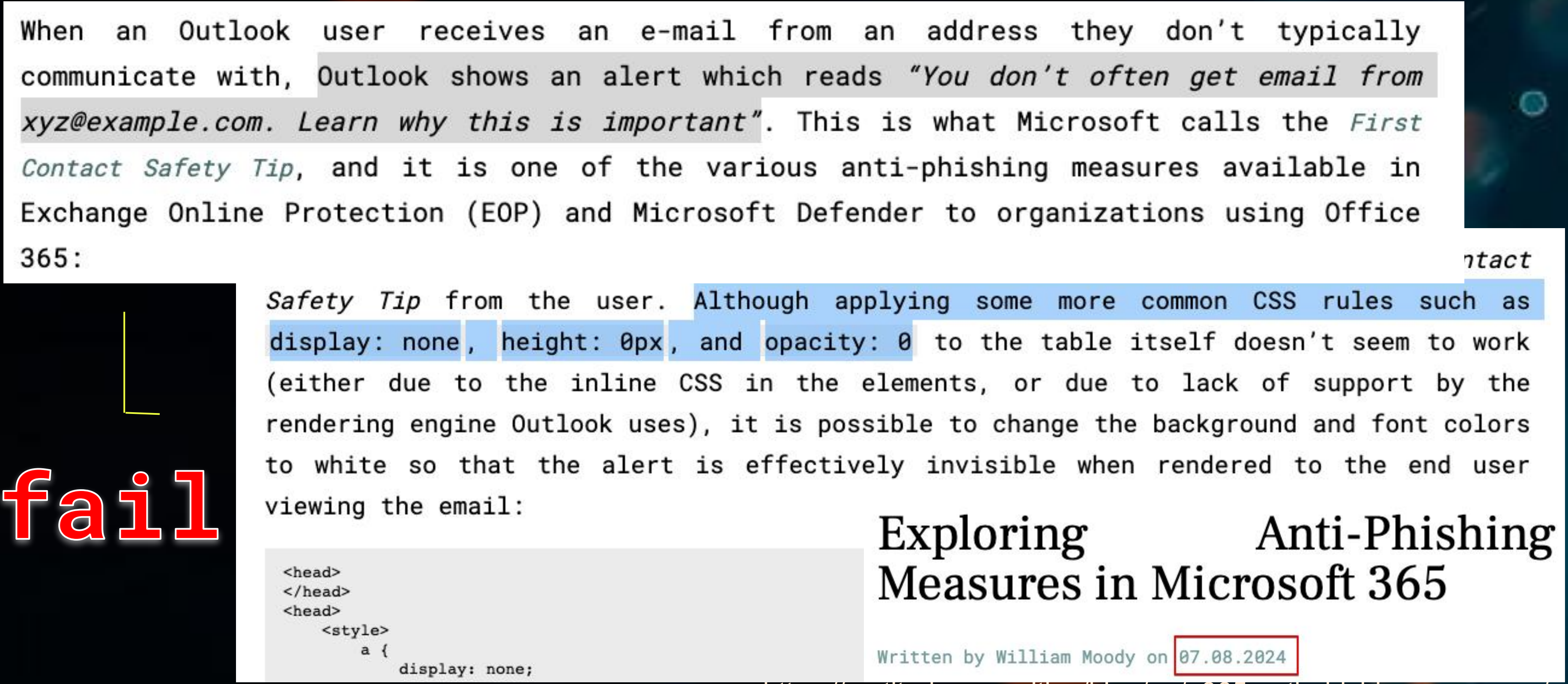
CVE-2024-29976 –

Five new vulnerabilities found in Zyxel NAS devices (including code execution and privilege escalation)

Research & Threat Intel · 04 Jun 2024

https://outpost24.com/blog/zyxel-nas-critical-vulnerabilities/

Защищай пользователя своего - Обход защиты



When an Outlook user receives an e-mail from an address they don't typically communicate with, Outlook shows an alert which reads *"You don't often get email from xyz@example.com. Learn why this is important"*. This is what Microsoft calls the *First Contact Safety Tip*, and it is one of the various anti-phishing measures available in Exchange Online Protection (EOP) and Microsoft Defender to organizations using Office 365:

ntact Safety Tip from the user. Although applying some more common CSS rules such as `display: none`, `height: 0px`, and `opacity: 0` to the table itself doesn't seem to work (either due to the inline CSS in the elements, or due to lack of support by the rendering engine Outlook uses), it is possible to change the background and font colors to white so that the alert is effectively invisible when rendered to the end user viewing the email:

```
<head>
</head>
<head>
    <style>
        a {
            display: none;
```

Exploring Anti-Phishing Measures in Microsoft 365

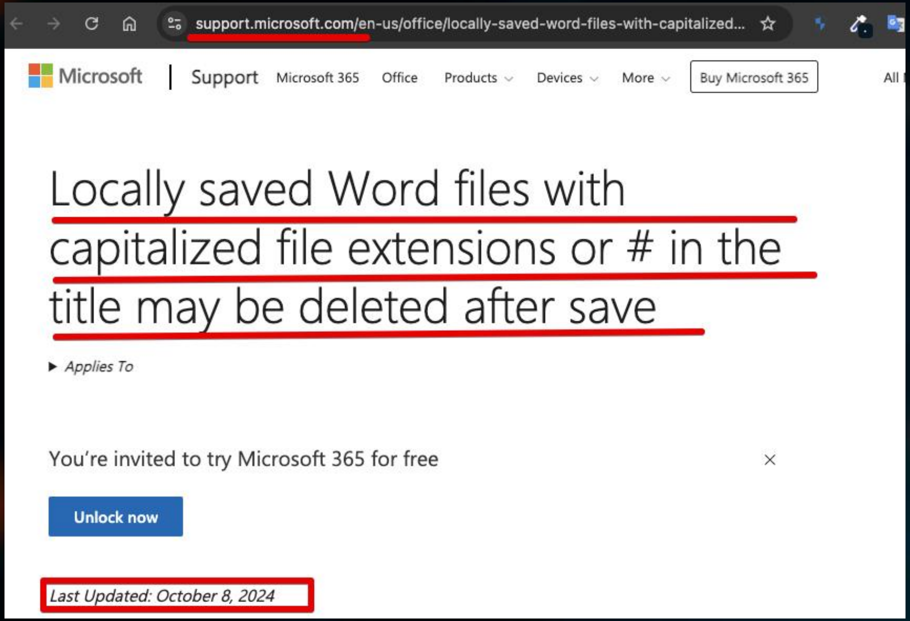
Written by William Moody on 07.08.2024

fail

https://certitude.consulting/blog/en/o365-anti-phishing-measures/

Когда сами продукты являются угрозой

fail



support.microsoft.com/en-us/office/locally-saved-word-files-with-capitalized...
Microsoft
Support
Microsoft 365
Office
Products
Devices
More
Buy Microsoft 365
All

Locally saved Word files with capitalized file extensions or # in the title may be deleted after save

▸ *Applies To*

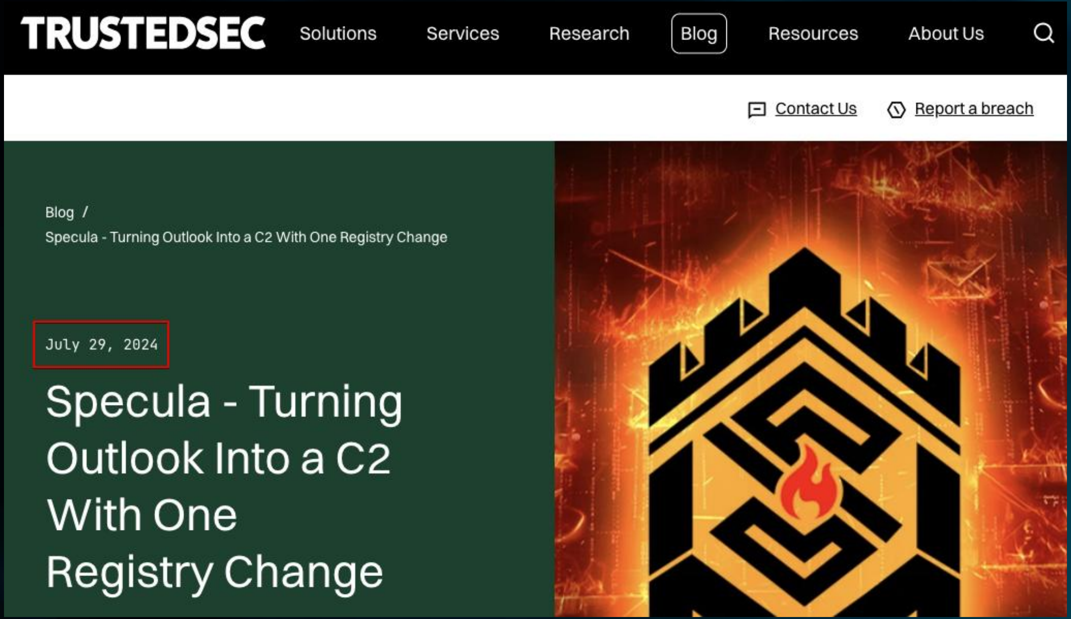
You're invited to try Microsoft 365 for free

Last Updated: October 8, 2024

https://support.microsoft.com/en-us/office/locally-saved-word-files-with-capitalized-file-extensions-or-in-the-title-may-be-deleted-after-save-5e28f8c2-32d0-487b-b237-9c7c74d25f84

Или становятся оружием

fail



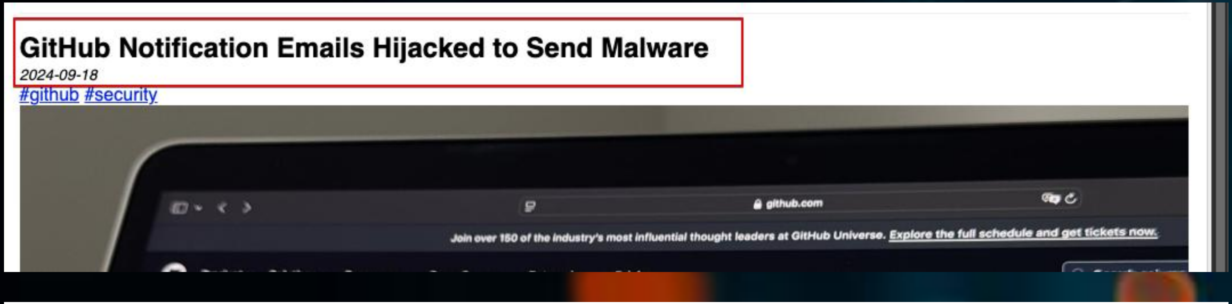
Blog /
Specula - Turning Outlook Into a C2 With One Registry Change

July 29, 2024

Specula - Turning Outlook Into a C2 With One Registry Change

https://trustedsec.com/blog/specula-turning-outlook-into-a-c2-with-one-registry-change

Рассылка малвари не дремлет

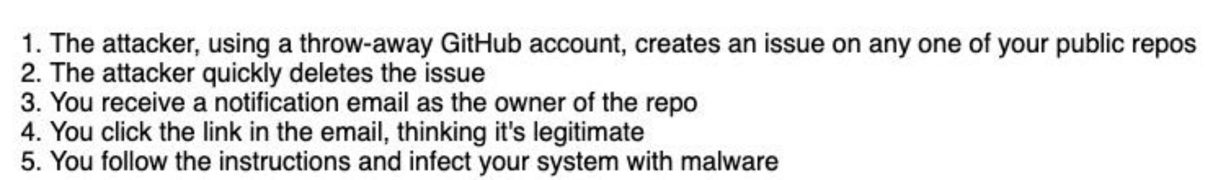


GitHub Notification Emails Hijacked to Send Malware

2024-09-18

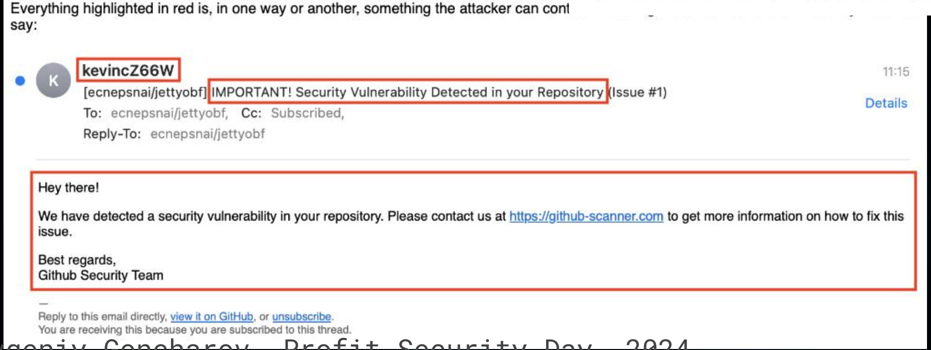
#github #security

github.com
Join over 150 of the industry's most influential thought leaders at GitHub Universe. Explore the full schedule and get tickets now.



1. The attacker, using a throw-away GitHub account, creates an issue on any one of your public repos
2. The attacker quickly deletes the issue
3. You receive a notification email as the owner of the repo
4. You click the link in the email, thinking it's legitimate
5. You follow the instructions and infect your system with malware

fail



Everything highlighted in red is, in one way or another, something the attacker can cont
say:

kevincZ66W

[ecnepsnai/jettyobf] IMPORTANT! Security Vulnerability Detected in your Repository (Issue #1)

To: ecnepsnai/jettyobf, Cc: Subscribed,

Reply-To: ecnepsnai/jettyobf

11:15

Details

Hey there!

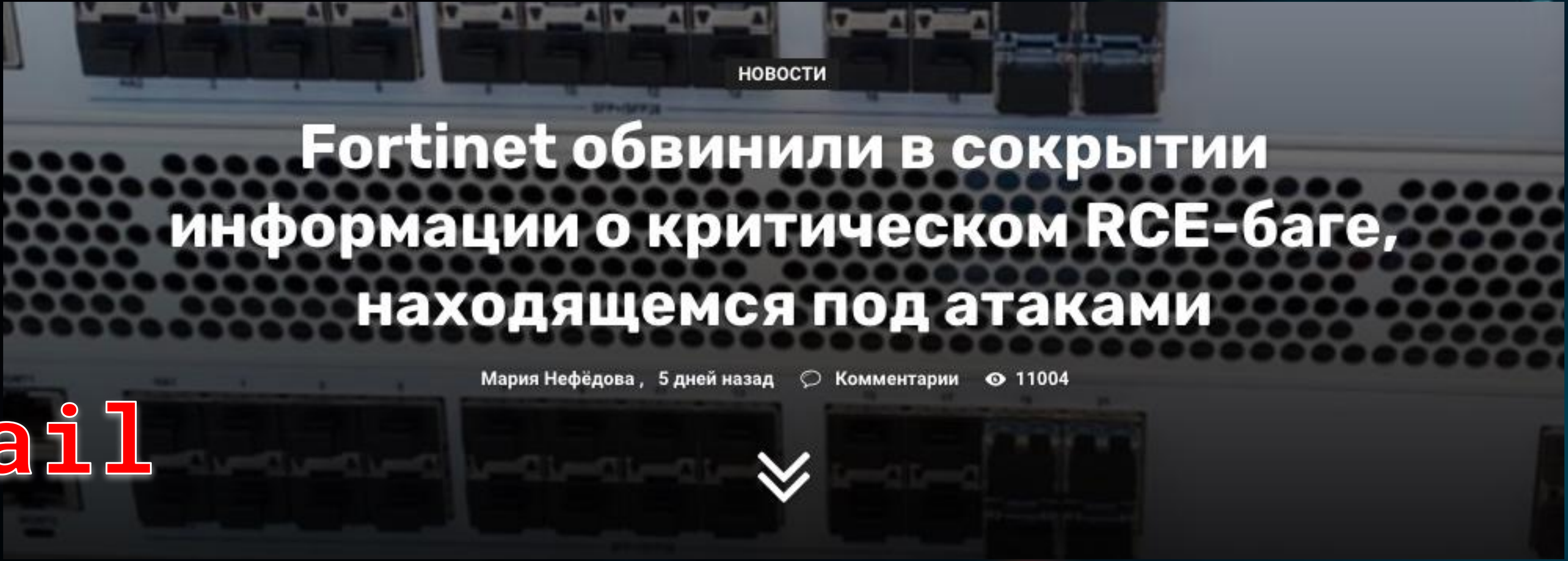
We have detected a security vulnerability in your repository. Please contact us at https://github-scanner.com to get more information on how to fix this issue.

Best regards,
Github Security Team

—
Reply to this email directly, view it on GitHub, or unsubscribe.
You are receiving this because you are subscribed to this thread.

https://ianspence.com/blog/2024-09/github-email-hijack/

Кто-то скрывает баги



НОВОСТИ

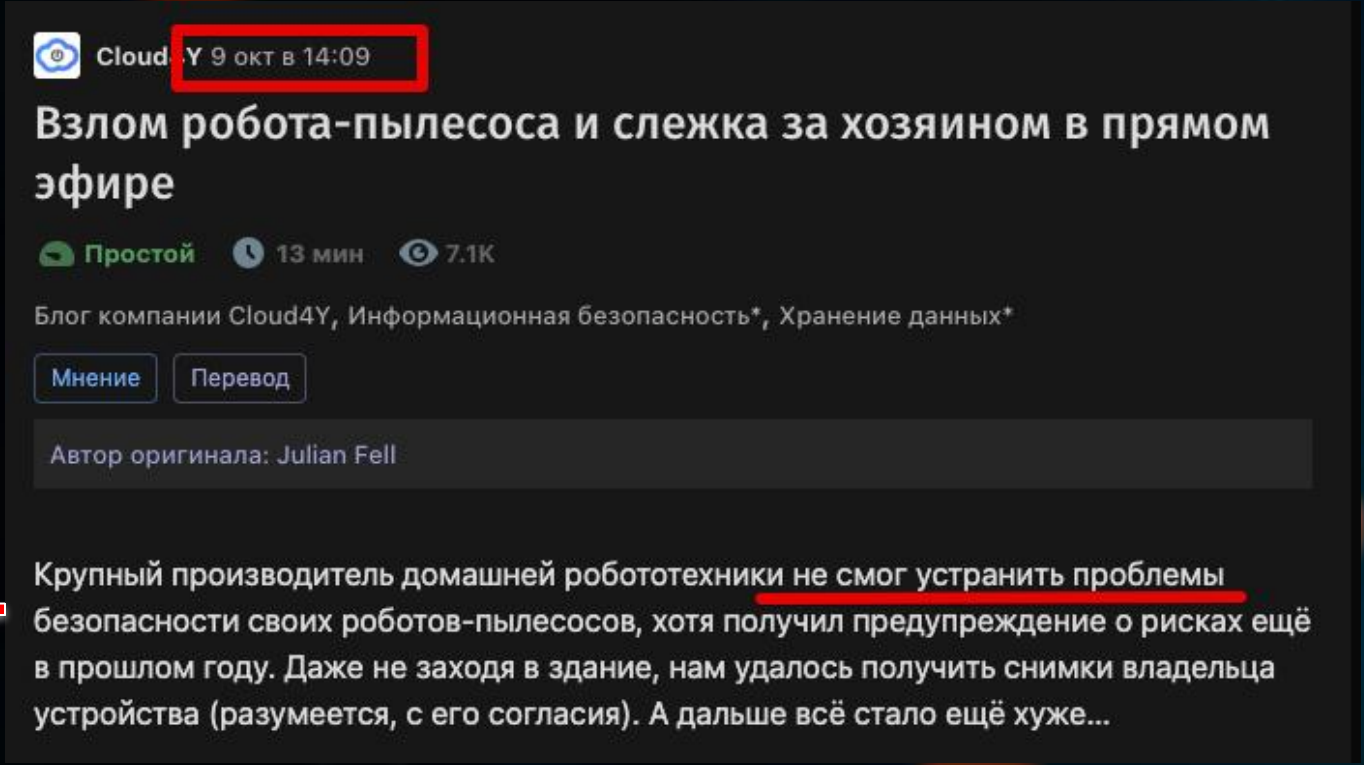
Fortinet обвинили в сокрытии информации о критическом RCE-баге, находящемся под атаками

Мария Нефёдова , 5 дней назад Комментарии 11004

fail

https://xakep.ru/2024/10/25/fortijump/

Можно следить при помощи пылесоса



Cloud4Y 9 окт в 14:09

Взлом робота-пылесоса и слежка за хозяином в прямом эфире

Простой 13 мин 7.1K

Блог компании Cloud4Y, Информационная безопасность*, Хранение данных*

Мнение Перевод

Автор оригинала: Julian Fell

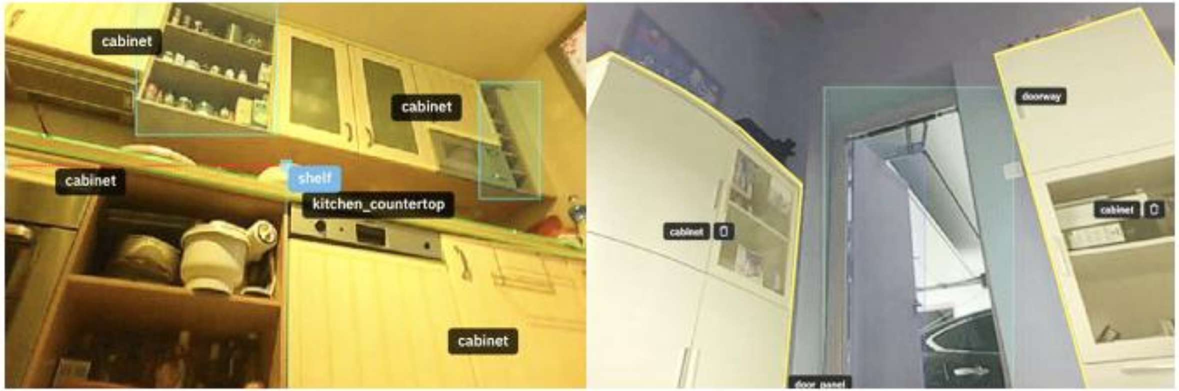
Крупный производитель домашней робототехники не смог устранить проблемы безопасности своих роботов-пылесосов, хотя получил предупреждение о рисках ещё в прошлом году. Даже не заходя в здание, нам удалось получить снимки владельца устройства (разумеется, с его согласия). А дальше всё стало ещё хуже...

fail

https://habr.com/ru/companies/cloud4y/articles/849294/

Не только следить, а вычленять планы и делать фото

Some of the leaked images captured

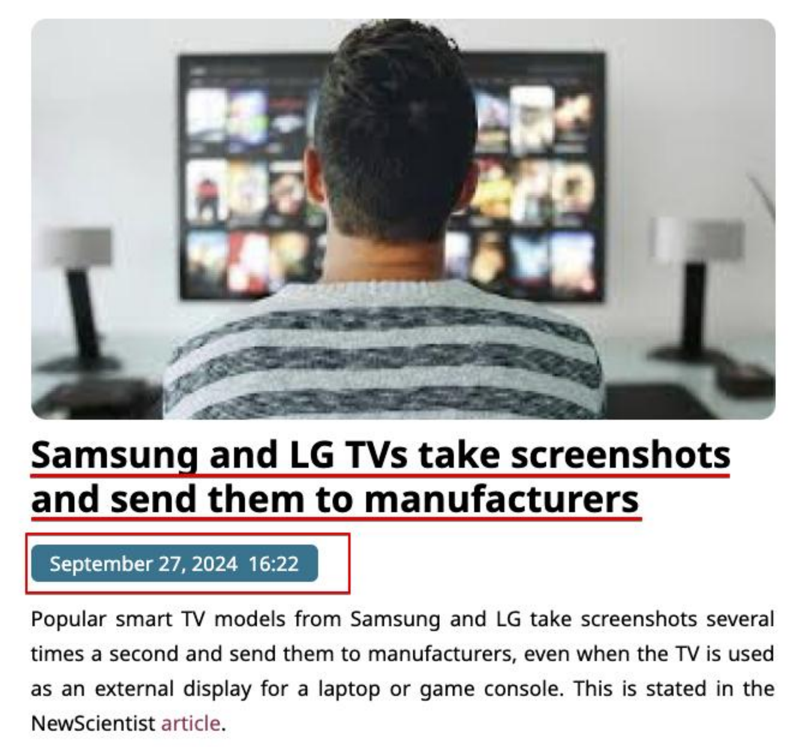


Images captured by iRobot development devices, being annotated by data labelers

fail

https://www.kaspersky.com/blog/robot-vacuum-privacy/46682/

И слать скрины с Твоего TV



Samsung and LG TVs take screenshots and send them to manufacturers

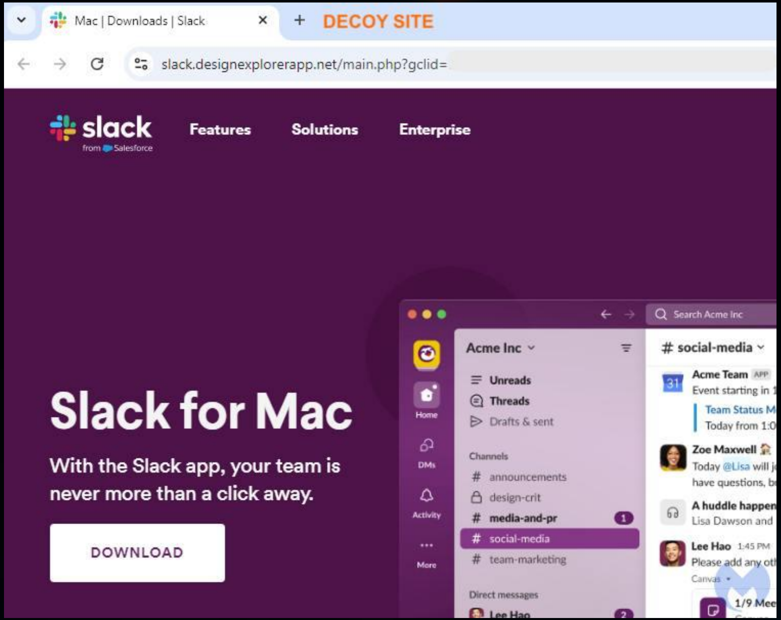
September 27, 2024 16:22

Popular smart TV models from Samsung and LG take screenshots several times a second and send them to manufacturers, even when the TV is used as an external display for a laptop or game console. This is stated in the NewScientist article.

fail

https://tech.news.am/eng/news/4348/samsung-and-lg-tvs-take-screenshots-and-send-them-to-manufacturers.html

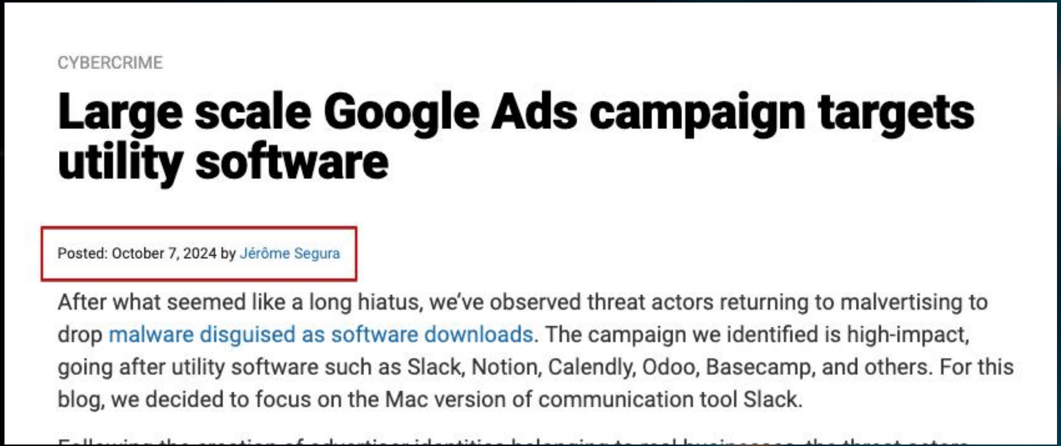
А софт с сюрпризом - рекламируется в поисковиках



Slack for Mac

With the Slack app, your team is never more than a click away.

DOWNLOAD



CYBERCRIME

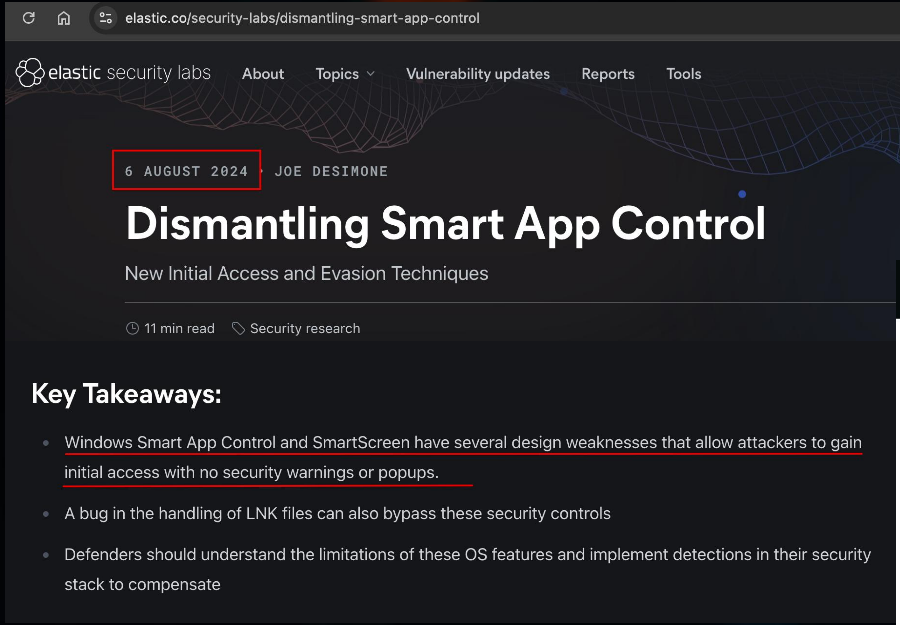
Large scale Google Ads campaign targets utility software

Posted: October 7, 2024 by Jérôme Segura

After what seemed like a long hiatus, we've observed threat actors returning to malvertising to drop malware disguised as software downloads. The campaign we identified is high-impact, going after utility software such as Slack, Notion, Calendly, Odoo, Basecamp, and others. For this blog, we decided to focus on the Mac version of communication tool Slack.

https://www.malwarebytes.com/blog/news/2024/10/large-scale-google-ads-campaign-targets-utility-softwarea

При этом можно попробовать обойти защиту AV



elastic.co/security-labs/dismantling-smart-app-control

6 AUGUST 2024 · JOE DESIMONE

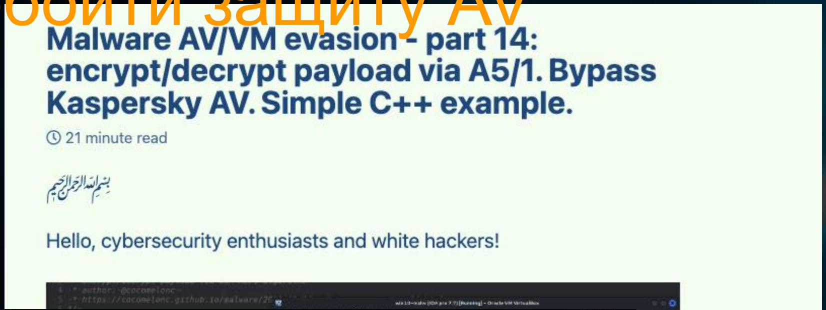
Dismantling Smart App Control

New Initial Access and Evasion Techniques

11 min read · Security research

Key Takeaways:

- Windows Smart App Control and SmartScreen have several design weaknesses that allow attackers to gain initial access with no security warnings or popups.
- A bug in the handling of LNK files can also bypass these security controls
- Defenders should understand the limitations of these OS features and implement detections in their security stack to compensate

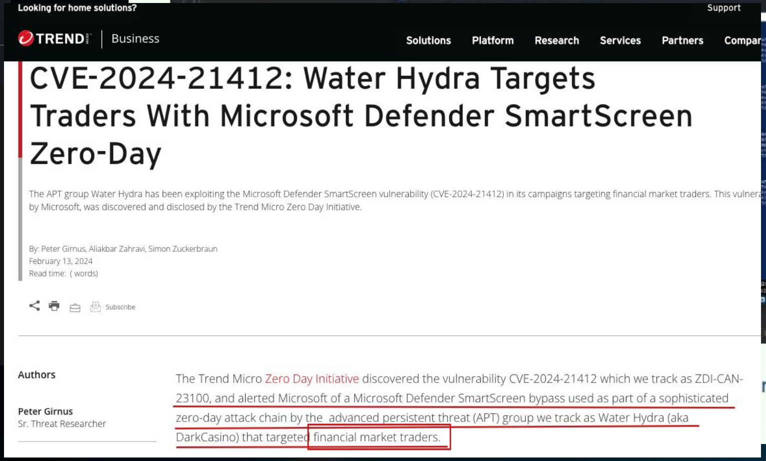


Malware AV/VM evasion - part 14: encrypt/decrypt payload via A5/1. Bypass Kaspersky AV. Simple C++ example.

21 minute read

بسم الله الرحمن الرحيم

Hello, cybersecurity enthusiasts and white hackers!



CVE-2024-21412: Water Hydra Targets Traders With Microsoft Defender SmartScreen Zero-Day

The APT group Water Hydra has been exploiting the Microsoft Defender SmartScreen vulnerability (CVE-2024-21412) in its campaigns targeting financial market traders. This vulnera by Microsoft, was discovered and disclosed by the Trend Micro Zero Day Initiative.

By: Peter Girnus, Aliakbar Zahravi, Simon Zuckerbraun
February 13, 2024
Read time: (words)

Subscribe

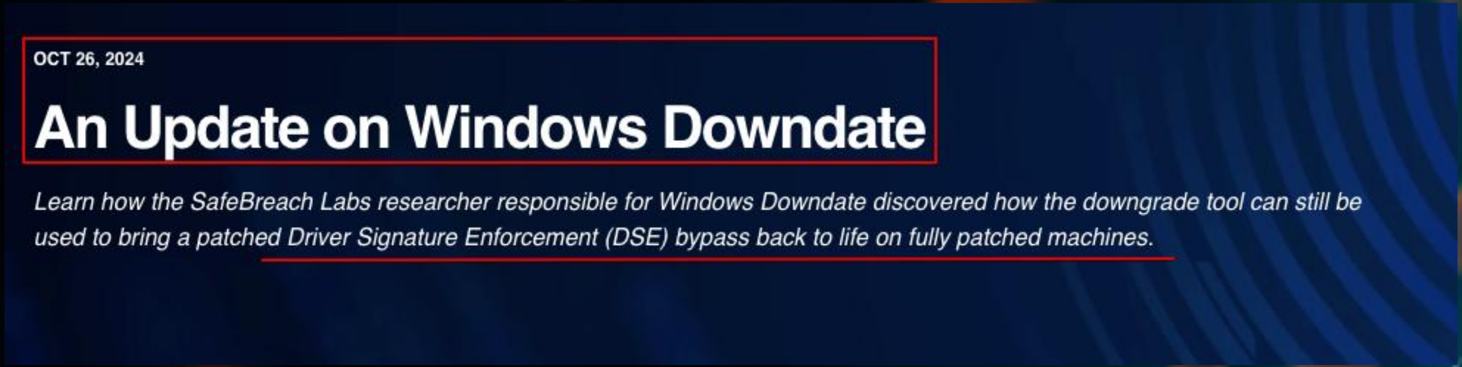
Authors

Peter Girnus
Sr. Threat Researcher

The Trend Micro Zero Day Initiative discovered the vulnerability CVE-2024-21412 which we track as ZDI-CAN-23100, and alerted Microsoft of a Microsoft Defender SmartScreen bypass used as part of a sophisticated zero-day attack chain by the advanced persistent threat (APT) group we track as Water Hydra (aka DarkCasino) that targeted financial market traders.

https://cocomelonc.github.io/malware/2023/03/24/malware-av-evasion-14.html,
https://www.elastic.co/security-labs/dismantling-smart-app-control,
https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html

Или внедрить старые уязвимости в полностью пропатченные системы



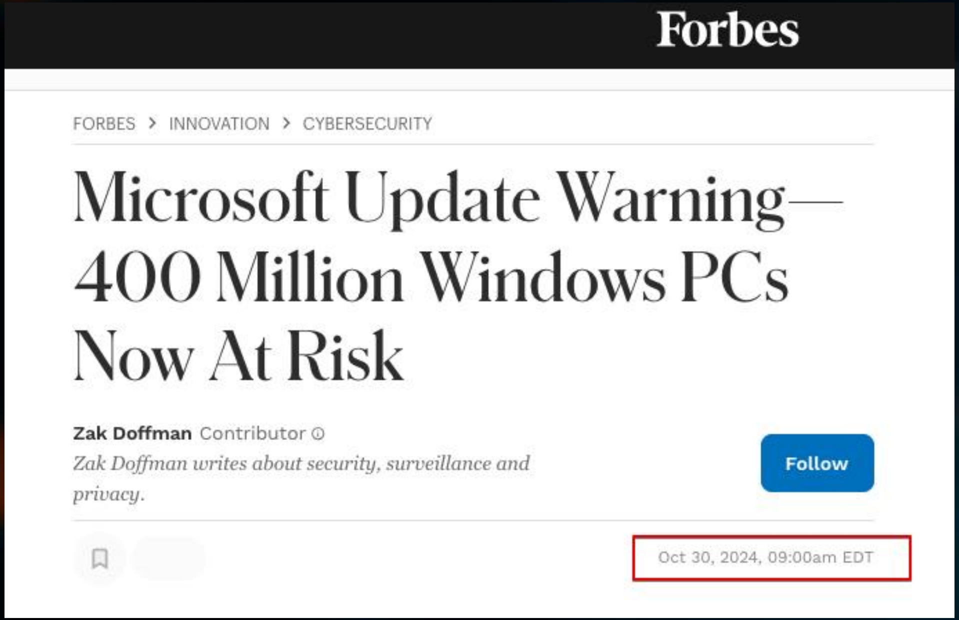
OCT 26, 2024

An Update on Windows Downdate

Learn how the SafeBreach Labs researcher responsible for Windows Downdate discovered how the downgrade tool can still be used to bring a patched Driver Signature Enforcement (DSE) bypass back to life on fully patched machines.

https://www.safebreach.com/blog/update-on-windows-downdate-downgrade-attacks/

Да и старые системы нужно обновлять



Forbes

FORBES > INNOVATION > CYBERSECURITY

Microsoft Update Warning—400 Million Windows PCs Now At Risk

Zak Doffman Contributor

Zak Doffman writes about security, surveillance and privacy.

Oct 30, 2024, 09:00am EDT

https://www.forbes.com/sites/zakdoffman/2024/10/30/warning-for-14-billion-microsoft-windows-10-windows-11-users-get-free-upgrade/

Немного о трендах

Тренды не покрывают всего ландшафта:

- https://www.cyberark.com/resources/ebooks/identity-security-threat-landscape-2024-report (17:00 - @sysadm_in_up)
- https://www.auratechnology.com/blog/7-most-common-cyberattack-vectors-in-2024/
- https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/

Помним - соц. инженерия, BEC, фейк - вакансии, партнеры, тест-задания

Как жи~~бы~~ть?

- Изыскивать проблемы и пробелы в своей защите
- Проводить awareness в своем окружении
- Изучать ресерчи - быть в курсе событий
- Не стоять на месте - развиваться
- Делиться опытом
- Изучать и пробовать новое

The End

- Yevgeniy Goncharov
- https://lab.sys-adm.in/
- https://www.linkedin.com/in/yevgeniy-goncharov/