From Dev to Security

Rey Bango (@reybango)
I would love to go to @defcon but I'm scared shitless to go to Def Con
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

1zt9YDgwueZ9NyMgw619p7AA8isjr6SMw
AppSec is hard
Note to developers:
It doesn't matter how "good" your password is if you tell everybody what it is.
“The attack was carried out by using a pattern that is becoming more and more popular; publishing a ‘useful’ package (electron-native-notify) to npm, waiting until it was in use by the target, and then updating it to include a malicious payload.”

Plot to steal cryptocurrency foiled by the npm sec...

Yesterday, the npm, Inc. security team, in collaboration with Komodo, helped protect over $13 million USD in cryptocurrency assets as we found and responded to ...

blog.npmjs.org

12:20 PM - 6 Jun 2019
This is exactly what many of us predicted when NPM introduced a world of thousands of separate dependencies per app. The main reactions to that skepticism were "stop being so negative" and "don't try to stop progress."

yan @bcrypt

“The attack was carried out by using a pattern that is becoming more and more popular: publishing a ‘useful’ package (electron-native-notify) to npm, waiting until it was in use by the target, and then updating it to include a malicious payload.” blog.npmjs.org/post/185397814...
Credit: https://imgur.com/user/PipePistoleer
OS maintainers differ in their code auditing cadence

- 26%: At least once a year
- 21%: At least once a quarter
- 21%: At least once a month
- 10%: Every couple of years or more
- 21%: We don’t
Implicit trust
How do you find about vulnerabilities?

- 36% I read the release notes of most of my direct and indirect dependencies
- 27% When my security team reports a severe vulnerability, we search for apps using this component
- 16% We track the list of dependencies against public databases (e.g. CVEs) ourselves
- 10% We use a dependency management/scanning tool that notifies us
- 9% Other
- 2% I probably won’t
On average, each Web application that Positive Technologies inspected contained **33 vulnerabilities**. Of those, six were high-severity flaws, compared to just two the prior year.

More than two-thirds of the apps **(67%) contained critical vulnerabilities such as insufficient authorization errors, arbitrary file upload, path traversal, and SQL injection flaws.**

https://www.darkreading.com/vulnerabilities---threats/web-apps-are-becoming-less-secure/
VeraCode polled 400 app developers from the UK, US and Germany and found just 52% update these components when a new vulnerability is announced. The research revealed that 83% of respondents use either commercial and/or open source components, with an average of 73 used per application.

Some 71 vulnerabilities per application are introduced on average through use of third-party components, with only 23% of respondents claiming they test for bugs in components at every release.

https://www.darkreading.com/vulnerabilities---threats/web-apps-are-becoming-less-secure/
Web apps & APIs are the new attack endpoints
Credit: Tanya Janca, Cloud Security Advocate at MSFT
Security Champions
Great question. I would summarize what I heard Ian say is that infosec needs to build bridges to better communicate with devops, which seems right. One of the major challenges, I find, is that developers often lack the perspective on the adversarial mindset.
The Complete Ethical Hacking Course for 2019!

Joseph Delgadillo 429K views • 4 months ago

Get the 19 course holiday bundle at https://josephdelgadillo.com/product/holiday-course-bundle-sale/ Get The Complete Ethical ...
Practice makes permanent
OWASP Juice Shop

https://www.owasp.org/index.php/OWASP_Juice_Shop_Project
Damn Vulnerable Web Application (DVWA)

http://www.dvwa.co.uk
OWASP DevSlop Project

https://www.owasp.org/index.php/OWASP_DevSlop_Project
Automate Security
BEFORE AUTOMATING YOUR OPEN SOURCE...

Over 75% were aware to only 50% of their open source inventory.

It takes 6 weeks on average to approve a new component.

90% have at least 1 vulnerability, over 45% have 5 and up.

There’s at least 1 license that doesn’t meet company policy on average.

* Based on first scan results for 250 applications and end of PoC questionnaire

Credit: WhiteSource.com
### Alerts

<table>
<thead>
<tr>
<th>Library</th>
<th>Type</th>
<th>Description</th>
<th>Occurrences</th>
<th>Creation Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>esapi-2.0.1.jar</td>
<td>Security Vulnerability</td>
<td>Medium: 1 (0) Low: 1</td>
<td>1 project details</td>
<td>07-05-2018</td>
<td>Ignore</td>
</tr>
<tr>
<td>bcpov-jdk15-1.4.6.jar</td>
<td>Security Vulnerability</td>
<td>Medium: 1 (0) details</td>
<td>1 project details</td>
<td>07-05-2018</td>
<td>Ignore</td>
</tr>
<tr>
<td>jackson-dataformat-xm...</td>
<td>Security Vulnerability</td>
<td>High: 1 (1)</td>
<td>1 project details</td>
<td>07-05-2018</td>
<td>Ignore</td>
</tr>
<tr>
<td>commons-beanutils-1.8...</td>
<td>Security Vulnerability</td>
<td>High: 1 (0)</td>
<td>5 projects</td>
<td>08-05-2018</td>
<td>Ignore</td>
</tr>
<tr>
<td>commons-fileupload-1...</td>
<td>Security Vulnerability</td>
<td>High: 4 (0) Low: 1 (0)</td>
<td>5 projects</td>
<td>08-05-2018</td>
<td>Ignore</td>
</tr>
<tr>
<td>spring-web-3.1.1.RELEASE</td>
<td>Security Vulnerability</td>
<td>Medium: 6 (0) details</td>
<td>5 projects</td>
<td>08-05-2018</td>
<td>Ignore</td>
</tr>
<tr>
<td>struts2-core-2.3.31.jar</td>
<td>Security Vulnerability</td>
<td>High: 2 (1) Medium: 3 (0)</td>
<td>5 projects</td>
<td>08-05-2018</td>
<td>Ignore</td>
</tr>
<tr>
<td>shiro-web-1.2.0.jar</td>
<td>Security Vulnerability</td>
<td>Medium: 1 (0)</td>
<td>5 projects</td>
<td>08-05-2018</td>
<td>Ignore</td>
</tr>
<tr>
<td>shiro-core-1.2.0.jar</td>
<td>Security Vulnerability</td>
<td>Medium: 1 (0)</td>
<td>5 projects</td>
<td>08-05-2018</td>
<td>Ignore</td>
</tr>
</tbody>
</table>

#### Security and Quality

- **Reported Vulnerability Score:** High
- **Libs. with Vulnerabilities:**
  - High: 9
  - Med: 18
- **Outdated and Vulnerable Libs.**
  - Outdated: 0
  - Out. & Vul.: 0
  - Vulnerable: 27
  - Critical: 0
  - Block: 0

#### Top 10 Products (8)

<table>
<thead>
<tr>
<th>Product</th>
<th>Projects</th>
<th>Libraries</th>
<th>Vulnerabilities</th>
<th>Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>appserver-working</td>
<td>1</td>
<td>296</td>
<td>High: 8 Medium: 21 Low: 25</td>
<td>25</td>
</tr>
<tr>
<td>appserver</td>
<td>1</td>
<td>291</td>
<td>High: 7 Medium: 19 Low: 14</td>
<td>14</td>
</tr>
<tr>
<td>Effective_Usage_Demo_1</td>
<td>1</td>
<td>41</td>
<td>High: 7 Medium: 13 Low: 8</td>
<td>8</td>
</tr>
<tr>
<td>Effective_Usage_Demo_2</td>
<td>1</td>
<td>41</td>
<td>High: 7 Medium: 13 Low: 8</td>
<td>8</td>
</tr>
<tr>
<td>ksa</td>
<td>1</td>
<td>41</td>
<td>High: 7 Medium: 13 Low: 8</td>
<td>8</td>
</tr>
<tr>
<td>Effective_Usage_Demo</td>
<td>1</td>
<td>41</td>
<td>High: 7 Medium: 13 Low: 8</td>
<td>8</td>
</tr>
<tr>
<td>My_WS_DemoEUA_Prod</td>
<td>1</td>
<td>40</td>
<td>High: 7 Medium: 13 Low: 8</td>
<td>8</td>
</tr>
</tbody>
</table>

#### License Distribution

- Eclipse 1.0
- GPL 2.0 Classpath
- LGPL 3.0
- GPL 2.0
- LGPL 2.1
- LGPL 2.0
- CDDL 1.0
- Apache 2.0
- Others
- Required

---
Build a strong network
Tanya Janca
@shehackspurple
Look for non-traditional talent
Do the right thing