Avenues of Exploitation
Use of Zero-Day Vulnerabilities by Tracked Groups

Jared Semrau
Senior Manager, Vulnerabilities and Exploitation

Parnian Najafi
Senior Analyst, Advanced Analysis

Kat Metrick
Analyst, Strategic Intelligence
Jared Semrau
Senior Manager, Vulnerabilities and Exploitation

- Background in cyber criminal monetization and money laundering analysis and threat analysis of vulnerability exploitation.

- Current focus on vulnerabilities, their exploitation, and high-level vulnerability trending.
Parnian Najafi
Senior Analyst, Advanced Analysis

- Background in vulnerability and IoT penetration testing
- Current focus on technical capabilities of threat actors
Kat Metrick
Analyst, Strategic Intelligence

- Background in Deep & Dark Web research
- Current focus on high level trends in state-sponsored and criminal activity
Key Questions
Key Questions

- What is a zero-day?
- Are zero-days a concern to me?
- Who is using them and why?
- How has zero-day usage changed over time?
- What can I do to protect my company?
Definitions and Methodology

What is a Zero-Day?
Definitions

- A zero-day vulnerability is a known flaw in software or hardware that leaves systems exposed to cyber attacks before a patch is available to properly mitigate the risk.
- For the purpose of this study, we focused on zero-days that had been actively exploited in the wild for malicious activity.
Data Sources

- FireEye original research
- Google Project Zero - 0day “in the wild” spreadsheet
- Open source collections
Historical Trends in Zero-Day Exploitation
Overall Trends: Zero-Days

- Spike in zero-day exploitation in 2019
- Breaks downward trend since 2016
- Important: number of vulnerabilities vs. breadth of exploitation
- Could be indication of shift in zero-day discovery rate
Decline in Exploit Kit Usage

- Zero-day exploits used to be observed regularly in exploit kits
- Successful law enforcement activity
  - Black Hole Exploit Kit
  - Angler Exploit Kit
- Most remaining developers either quit, or established more exclusive relationships
- Since 2017, no new zero-days in exploit kits
Other Factors Leading to Decline

- Decreased viability of browser-based attacks:
  - Increased default security settings in Java shakes up targeting in 2013
  - Default automatic browser updates introduced
  - Looming Flash end-of-life

- Shift in actor tactics
  - Financially motivated actors increasingly performing targeted attacks, requiring different exploits
  - Increased use of exploit document builders, one-day exploits, and macros
Zero-Day targeting of obscure software is rare

- Actors want most bang for their buck
- Common software provides widest potential attack surface

Over 75% of all zero-days are Microsoft or Adobe
Products Affected by Zero-Days

- Same story as vendors...
- A handful of products account for the vast majority of zero-day activity
Current State of Zero-Day Landscape in 2019
Significant Shift in Capabilities

- Zero-days used to be the exclusive property of the most sophisticated state and criminal actors
- New groups display access (FIN6, SandCat)
- Increased commodification of zero-days
  - Bug bounty programs and private security firms
  - Some companies suspected of selling zero-days to actors
  - Helps to explain recent spike in discovery rate
Less Significance of Access

- Access to zero-days as a measure of threat actor sophistication
- Effect of rise of private security firms and bug bounty programs on sophistication measurement
- Exploit development speed for a known vulnerability as a measure of sophistication
Recognition vs. Financial Incentives

- Actors capable of discovering zero-days have competing interests
  - Recognition/ bragging rights
  - Financial gain

- Other factors:
  - Nationalization of zero-days
Zero-Day Usage by Tracked Groups
Zero-Day Usage CVEs Assigned 2012-2019

APT28

Fruity Armor/Stealth Falcon

APT26

Black Oasis

APT17

APT19

APT20

APT3

APT18

FIN6

APT22

Hermit

FIN8

Turla

Sand Cat

APT31

Buckeye

Dark Hotel

Animal Farm

Mana

>10 5-10 4-2 1
Zero-Day Usage by Country

- **US**: 7 zero-days
- **France**: 1 zero-day
- **Uzbekistan**: 3 zero-days
- **Russia**: 14 zero-days
- **China**: 19 zero-days
- **North Korea**: 3 zero-days
Zero-Day Usage, CVEs Assigned 2012-2015

APT17

APT26

APT28

APT3

APT19

APT20

APT18

Platinum

Mana

Hurricane Panda

Sand worm

Hermit
Zero-Day Usage, CVEs Assigned 2016-2019

- Stealth Falcon/Fruity Armor
- Buckeye
- Black Oasis
- APT31
- Sand Cat
- APT28
- FIN8
- FIN6
- APT37
- Turla
- FIN6
- FIN8
- APT31
- Buckeye
- Stealth Falcon/Fruity Armor
Notable APT Groups
2016-2019

- FruityArmor/Stealth Falcon
- SandCat
- BlackOasis
## Case Study: Time to Exploit

### CVE Release Date vs. Date of APT37 CVE Exploitation

| Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 2016 |     |     |     |     |     |     |     |     |     |     |     | 2017 |     |     |     |     |     |     |     |     |     |     |     |

- **CVE-2016-4117**
- **CVE-2017-0199**

- CVE Release Date
- Exploit
Zero-Day vs. Public Exploit or POC Availability

- Exploit, POC or Both Available
- No Exploit or PoC
Most Affected Vendors by Tracked Groups

- 78% of Global Markets use Microsoft operating system vs. 14% using Apple
Most Affected Products by Tracked Groups

ZERO-DAY PERCENTAGE IN PRODUCTS

- Java
- Internet Explorer
- Flash
- Windows Server
- Office
- Word
- Silverlight
- iOS
- Windows Server
Implications

What are the Key Takeaways?
The Who and Why Matters

- Knowing who is targeting you and why matters!
- Even if you can’t stop the zero-day, understanding their lifecycle can help you prepare to stop them elsewhere
Potential Shift in Capabilities

- More zero-days, but also more targeted use
  - Likelihood of being targeted has gone down, but activities are still as damaging as ever
  - Even if spike doesn’t continue, we should still be prepared
- Increased commodification changes how we view sophistication of groups
Patch Preparedness

- Can’t predict zero-days, but can be prepared
  - Patch commonly targeted vendors and products (Microsoft and Adobe)
- Notable breaches have taught us that exploitation impacts everyone
  - Everyone needs to share the responsibility
- Prioritize active threats first
  - Limited patching resources require efficiency
  - Active Threat → Potential Threat → No Known
  - Ignore CVSS scores and branded vulnerabilities
Questions?
Thank You!