The Shadow Brokers

AN OVERVIEW OF THE WANNACRY GLOBAL RANSOMWARE ATTACK

By Zach Weaver

Introduction

- Hacking group that first emerged in 2016
- Known for leaking classified NSA hacking tools and other exploits of some of the most dangerous malware attacks
- They have had a significant impact on the cybersecurity landscape

History

- First publicly emerged in 2016
- Operated under the twitter handle @shadowbrokerss
- Name comes from a MassEffect video game character
- First public communication was when they auctioned off a suite of stolen hacking tools in exchange for 100 Bitcoins
- Some researchers allegedly believe they were affiliated with the Russian government

Targets and Motivations

- Main goal was to leak classified hacking information used by the NSA
- They claimed they were committed to taking down the NSA
- Targeted the Equation Group (offensive cyberwarfare unit of the NSA Computer Network Operations unit)

Equation Group

Equation Group was the Informal Name of the Tailored Access Operations (TAO) unit of the US’s National Security Agency (NSA)

Active since 1996 but gained popularity in 2008

Linked with various branches of the NSA

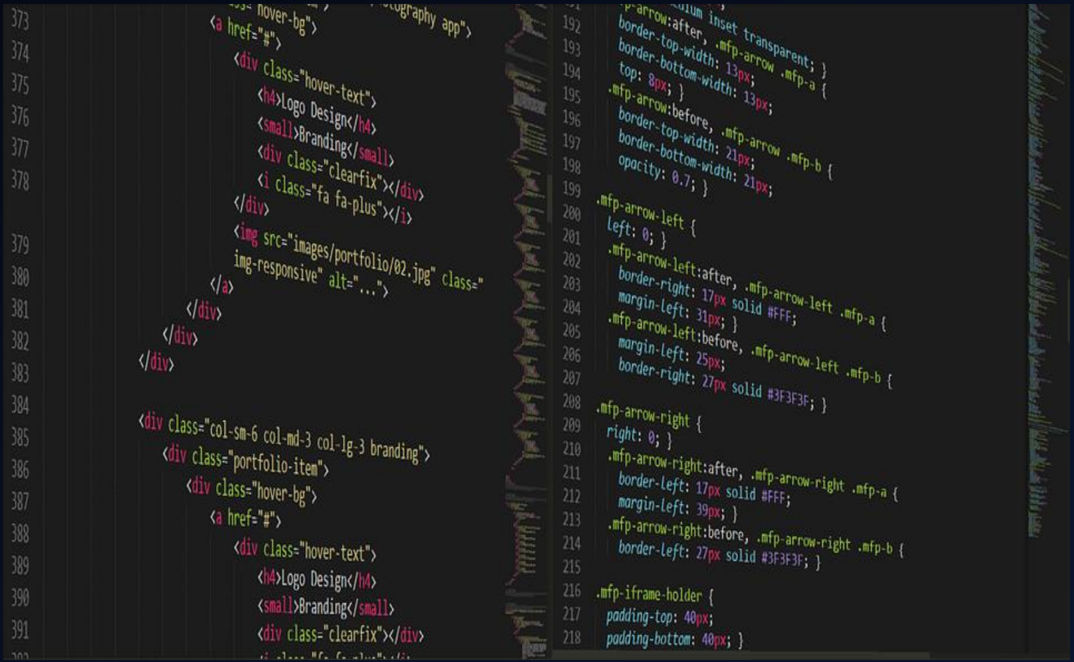
EG Thought to be behind the Stuxnet worm that disrupted Iran’s nuclear program

Allegedly responsible for developing incredible cyber weapons

Group was considered a secret until the Shadow Brokers came along in 2016

Notable Attacks – WannaCry

- Ransomware attack that encrypted files of victims in over 150 countries
- Shadow Brokers Held an auction for tools used by the Equation Group (EternalBlue, Eternal Romance, other exploits)
- Offered a “data dump of the month” to anyone willing to pay
- Released NSA tools onto the internet (including attack campaigns from 2000 – 2013)



```
            <a href="#">
                <div class="hover-text">
                    <h4>Logo Design</h4>
                    <small>Branding</small>
                    <div class="clearfix"></div>
                    <i class="fa fa-plus"></i>
                </div>
                <img src="images/portfolio/02.jpg" class="
                img-responsive" alt="...">
            </a>
        </div>
    </div>
</div>

<div class="col-sm-6 col-md-3 col-lg-3 branding">
    <div class="portfolio-item">
        <div class="hover-bg">
            <a href="#">
                <div class="hover-text">
                    <h4>Logo Design</h4>
                    <small>Branding</small>
                    <div class="clearfix"></div>
```

```
    border-top-width: 13px;
    border-bottom-width: 13px;
    top: 8px; }
  .mfp-arrow:before, .mfp-arrow .mfp-b {
    border-top-width: 21px;
    border-bottom-width: 21px;
    opacity: 0.7; }
.mfp-arrow-left {
  left: 0; }
  .mfp-arrow-left:after, .mfp-arrow-left .mfp-a {
    border-right: 17px solid #FFF;
    margin-left: 31px; }
  .mfp-arrow-left:before, .mfp-arrow-left .mfp-b {
    margin-left: 25px;
    border-right: 27px solid #3F3F3F; }
.mfp-arrow-right {
  right: 0; }
  .mfp-arrow-right:after, .mfp-arrow-right .mfp-a {
    border-left: 17px solid #FFF;
    margin-left: 39px; }
  .mfp-arrow-right:before, .mfp-arrow-right .mfp-b {
    border-left: 27px solid #3F3F3F; }

.mfp-iframe-holder {
  padding-top: 40px;
  padding-bottom: 40px; }
```

Eternal Blue

- Windows exploit created by the NSA
- Exploits a vulnerability in the Microsoft SMB protocol
- Caused unpatched Windows machines to allow illegitimate data packets into a legitimate network (containing malware)
- NSA did not alert Microsoft about EternalBlue’s existence for five years (until data leak)

Responses and Consequences

- Shadow Brokers appeared to have unrestricted access to the NSA
- Went on to reveal many servers and tools used by the Equation Group
- Edward Snowden speculated that they conduced a “reverse hack” using Eternal Blue and similar tools (backdoor into NSA)
- Microsoft went on to share a security patch for Windows sysadmins
- Since the initial attack, the Shadow Brokers have gone silent
- Origins and Identities still unknown

References

- https://www.hypr.com/security-encyclopedia/shadow-brokers
- https://securityscorecard.com/blog/what-is-equation-group-shadow-brokers/
- https://www.avg.com/en/signal/the-most-dangerous-hackers-today
- https://www.microsoft.com/en-us/security/blog/2017/06/16/analysis-of-the-shadow-brokers-release-and-mitigation-with-windows-10-virtualization-based-security/