Is the Damage Already Done?

Automating Vulnerability Investigation

John Moran – Senior Product Manager, DFLabs
Overview.

- Vulnerability exploitation and timeline
- CVE-based intelligence
- Going back in time
- Implementing with automation
Vulnerability Exploitation

The Etiology of Vulnerability Exploitation – RSA 2019
Jay Jacobs (Cyentia Institute) and Michael Roytman (Kenna Security)

- CVEs and publicly available exploit databases
- Data from scanners and IPS/IDS systems (a total of 7.3 billion attack records and 2.8 billion vulnerabilities in 13 million systems)

https://youtu.be/h_HdKzsfxmg
CVE › Exploit.

Source: Kenna / Cyentia
Vulnerability Timeline.

From Exploit to Patch

Day 0

CVE & Exploit
Vulnerability Timeline

From Exploit to Patch

Day 0 - CVE & Exploit
Day 3 - Signature Available
Vulnerability Timeline.

From Exploit to Patch

- Day 0: CVE & Exploit
- Day 3: Signature Available
- Day 7: Patch Available
Vulnerability Timeline.

From Exploit to Patch

Day 0: CVE & Exploit
Day 3: Signature Available
Day 7: Patch Available

...? Patched

Vulnerability Timeline.

From Exploit to Patch

Day 0
- CVE & Exploit

Day 3
- Signature Available

Day 7
- Patch Available

...?
- Patched
IF I COULD
TURN BACK TIME
CVE Intel

```json
{
  data: {
    results: [
      {
        relatedLinks: [
          "http://www.securitytracker.com/id/1040153",
          ...
        ],
        ...
      },
      risk: {
        criticalityLabel: "Very Critical",
        score: 99,
        evidenceDetails: [
          ...
        ],
        cvssv3: {
          scope: "UNCHANGED",
          integrityImpact: "HIGH",
          exploitabilityScore: 1.8,
          modified: "2018-03-16T16:09:27.543Z",
          version: "3.0",
          baseSeverity: "HIGH",
          baseScore: 7.8,
          privilegesRequired: "NONE",
          userInteraction: "REQUIRED",
          impactScore: 5.9,
          attackVector: "LOCAL",
          attackComplexity: "LOW",
          created: "2018-01-10T01:29:00.820Z",
          availabilityImpact: "HIGH"
        },
        ...
      }
    ],
    counts: {
      returned: 1,
      total: 1
    }
  }
}
```
"CVE Intel.

hash:1c633806de81c9181da572ce40e32254"
CVE Intel.

```json
{
  data: {
    results: {
      relatedLinks: [
        "http://www.securitytracker.com/id/1040153",
      ],
      ...,
      risk: {
        criticalityLabel: "Very Critical",
        score: 99,
        evidenceDetails: [
          ...
        ],
        cvssv3: {
          scope: "UNCHANGED",
          integrityImpact: "HIGH",
          exploitabilityScore: 1.8,
          modified: "2018-03-16T16:09:27.543Z",
          version: "3.0",
          baseSeverity: "HIGH",
          baseScore: 7.8,
          privilegesRequired: "NONE",
          userInteraction: "REQUIRED",
          impactScore: 5.9,
          attackVector: "LOCAL",
          attackComplexity: "LOW",
          created: "2018-01-10T01:29:00.820Z",
          availabilityImpact: "HIGH"
        },
        ...,
        cvss: {
          accessVector: "NETWORK",
          lastModified: "2018-03-16T16:09:27.543Z",
          published: "2018-01-10T01:29:00.820Z",
          score: 9.3,
          availability: "COMPLETE",
          confidentiality: "COMPLETE",
          version: "2.0",
          authentication: "NONE",
          accessComplexity: "MEDIUM",
          integrity: "COMPLETE"
        },
      ],
      counts: {
        returned: 1,
        total: 1
      }
    },
    entity: {
      id: "U_3qAY",
      name: "CVE-2018-0802",
      type: "CyberVulnerability",
      description: "Equation Editor in Microsoft Office 2007..."
    },
    ...,
    entity: {
      id: "hash:1c633806de81c9181da572ce40e32254",
      name: "1c633806de81c9181da572ce40e32254",
      type: "Hash"
    },
    ...,
    entity: {
      id: "ip:118.189.81.19",
      name: "ip:118.189.81.19",
      type: "IpAddress"
    },
    ...,
    entity: {
      id: "idn:umumi.xyz",
      name: "umumi.xyz",
      type: "InternetDomainName"
    },
    ...,
    ...,
  },
  ...,
  ip:118.189.81.19
}```
idn:umumi.xyz
Turn Back Time.

Combine CVE intelligence with EDR, Netflow and SIEM data to detect previously exploited vulnerabilities.

YEAH...

I'M WAY TOO BUSY
Turn Back Time.

Searching Manually

```json
{
  data: {
    results: [ {
      relatedLinks: [ { "http://www.securitytracker.com/id/1040153" } ],
      risk: { criticalityLabel: "Very Critical", score: 99, evidenceDetails: [ ] },
    counts: { returned: 1, total: 1 } }
```
Thank You.

Any Questions?

dflabs.com

linkedin.com/in/johntmoran