There Can Be Only One!: Last CTI Vendor Standing Pitch

Moderator: John Pescatore, Director, SANS Institute
Mark Kendrick, DomainTools
Matt Kodama, RecordedFuture
Jess Parnell, Centripetal Networks
Roselle Safran, UpLevel Security
There Can Be Only One!: Last CTI Vendor Standing Pitch

Mark Kendrick, DomainTools
See Threats Coming

DETECT | INVESTIGATE | PREVENT
DomainTools Iris

Welcome to DomainTools Iris. From here, you can open an existing investigation, create a new one, or simply begin searching.

Note: Input your terms to start a new investigation.
<table>
<thead>
<tr>
<th>Domain</th>
<th>Risk Score</th>
<th>Email</th>
<th>Email Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>pdfpump.net</td>
<td>20.42</td>
<td>Address</td>
<td>privacyprotect.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:contact@privacyprotect.org">contact@privacyprotect.org</a></td>
<td>publicdomainregistry.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:abuse-contact@publicdomainregistry.com">abuse-contact@publicdomainregistry.com</a></td>
<td>Whois</td>
</tr>
<tr>
<td>Domain</td>
<td>Registrar Status</td>
<td>Create Date</td>
<td>Expiration Date</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>pdfpump.net</td>
<td>COM</td>
<td>2015-10-15 (97 days old)</td>
<td>2016-10-15 (in 9 months)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>Registrar Status</td>
<td>Create Date</td>
<td>Expiration Date</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>pdfpump.net</td>
<td>clientTransferProhibited</td>
<td>2015-10-15</td>
<td>2016-10-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(97 days old)</td>
<td>(in 9 months)</td>
</tr>
</tbody>
</table>

**Filters**
- Narrow Search
- Expand Search
- New Search
- Exclude

**IP Tools**
- IP Profile
- Ping
- Traceroute
- PTR

~ 3 domains share this value.
<table>
<thead>
<tr>
<th>Domain</th>
<th>Risk Score</th>
<th>Email</th>
<th>Type(s)</th>
<th>Email Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>pdfpump.com</td>
<td>20.42</td>
<td>Address</td>
<td></td>
<td>kvaz.com publicdomain</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:link@kvaz.com">link@kvaz.com</a></td>
<td>Admin, Registrant, Technical</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:abuse-contact@publicdomainregistry.com">abuse-contact@publicdomainregistry.com</a></td>
<td>Whois</td>
<td></td>
</tr>
<tr>
<td>pdfpump.net</td>
<td>20.42</td>
<td>Address</td>
<td></td>
<td>privacyprotect publicdomain</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:contact@privacyprotect.org">contact@privacyprotect.org</a></td>
<td>Admin, Registrant, Technical</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:abuse-contact@publicdomainregistry.com">abuse-contact@publicdomainregistry.com</a></td>
<td>Whois</td>
<td></td>
</tr>
<tr>
<td>pdfpump.org</td>
<td>16.67</td>
<td>Address</td>
<td></td>
<td>privacyprotect publicdomain</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:contact@privacyprotect.org">contact@privacyprotect.org</a></td>
<td>Admin, Registrant, Technical</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>Risk Score</td>
<td>Email Address</td>
<td>Type(s)</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>--------------------</td>
<td>-------------------------------</td>
<td></td>
</tr>
<tr>
<td>pdfpump.com</td>
<td>20.42</td>
<td><a href="mailto:link@kvaz.com">link@kvaz.com</a></td>
<td>Admin, Registrant, Technical</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>kvaz.com publicdomain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>publicdomain</td>
<td></td>
</tr>
<tr>
<td>pdfpump.net</td>
<td>20.42</td>
<td><a href="mailto:contact@privacyprotect.org">contact@privacyprotect.org</a></td>
<td>Admin, Registrant, Technical</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>privacyprotect publicdomain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>publicdomain</td>
<td></td>
</tr>
<tr>
<td>pdfpump.org</td>
<td>16.42</td>
<td><a href="mailto:contact@privacyprotect.org">contact@privacyprotect.org</a></td>
<td>Admin, Registrant, Technical</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>privacyprotect publicdomain</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>publicdomain</td>
<td></td>
</tr>
</tbody>
</table>

- **Filters**
  - Narrow Search
  - Expand Search
  - New Search
  - Exclude

- ~380 domains share this value.
<table>
<thead>
<tr>
<th>Domain</th>
<th>Risk Score</th>
<th>Email</th>
<th>Email Domain</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>hasanweb.org</td>
<td>100</td>
<td><a href="mailto:link@kvaz.com">link@kvaz.com</a></td>
<td>123server.jp</td>
<td>Name: Aleks Kocyubenko Organization: Druzh Schaste. Address: UA</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:jp-info@123server.jp">jp-info@123server.jp</a></td>
<td>kvaz.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS/SoA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lafrenierre.net</td>
<td>54.04</td>
<td><a href="mailto:link@kvaz.com">link@kvaz.com</a></td>
<td>godaddy.com</td>
<td>Name: Aleks Kotsyubenko Organization: kv. Energ Schaste, UA</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:hostmaster@domainit.com">hostmaster@domainit.com</a></td>
<td>kvaz.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS/SoA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:abuse@godaddy.com">abuse@godaddy.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Whois</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nnvsu.com</td>
<td>54.04</td>
<td><a href="mailto:link@kvaz.com">link@kvaz.com</a></td>
<td>godaddy.com</td>
<td>Name: Aleks Kotsyubenko Organization: kv. Energ Schaste, UA</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:webmaster@hastydns.com">webmaster@hastydns.com</a></td>
<td>kvaz.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:abuse@godaddy.com">abuse@godaddy.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Whois</td>
<td></td>
<td></td>
</tr>
<tr>
<td>denniswolfe.com</td>
<td>54.04</td>
<td><a href="mailto:link@kvaz.com">link@kvaz.com</a></td>
<td>godaddy.com</td>
<td>Name: Aleks Kotsyubenko Organization: kv. Energ Schaste, UA</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:abuse@opticaljungle.com">abuse@opticaljungle.com</a></td>
<td>kvaz.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS/SoA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:abuse@godaddy.com">abuse@godaddy.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Whois</td>
<td></td>
<td></td>
</tr>
<tr>
<td>seljo.org</td>
<td>54.04</td>
<td><a href="mailto:link@kvaz.com">link@kvaz.com</a></td>
<td>bih.net.ba</td>
<td>Name: Aleks Kotsyubenko Organization: kv. Energ Schaste, UA</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:akkus@bih.net.ba">akkus@bih.net.ba</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS/SoA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:info@parallels.com">info@parallels.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Iris Overview

USE CASES

• Got Behind Privacy by Leveraging Attached Infrastructure (NSIP)
• Uncovered Who Owned the Domain
• Uncovered the Domains Connected to the Same Actor

• Proactively block access
• Search For Domains in Network Logs (DNS, Proxy, etc)
• Study Infrastructure
• Monitor Future Registrations
Methodology & Process

- BLOCK IT
- BLOCK OTHERS
- STRENGTHEN DEFENSES
- PROACTIVELY BLOCK

1. Assess Risk
2. Map Threats
3. Who?
4. Track

DOMAIN OR IP ADDRESS

Profile
Enumerate
Attribute
Monitor

Automate

Business Value
SOC Process
DomainTools Methodology
See Threats Coming

DETECT | INVESTIGATE | PREVENT

sales@domaintools.com
There Can Be Only One!: Last CTI Vendor Standing Pitch

Matt Kodama, RecordedFuture
Threat Intelligence Kumite!

SANS CTI Summit 2016
Matt Kodama, VP Products
Threat Intelligence Capability Wish List

- Works for TI teams like us
- Versatile for many TI problems
- Enhances current TI methods
- Improves our defensive controls
- Empowers other security teams
- Informs strategic decisions
Index
in real-time.
Organize for threat research.

OPs
IOCs
Events
Authors
Malware
Locations
Technologies
Product names
Company names
Actor/group names
+140 more features
Works for Threat Intel teams like us

• Delivers value immediately
• Usable by novice analysts
• Precision targeting for ninjas
• Durable through turnover
Versatile for many Threat Intel problems

- Many internal customers
- Evolving IT environment
- New vulnerabilities
- New actors and TTPs
Enhances my current Threat Intel methods

- Internal telemetry
- DHS, CERT, ISAC
- Trusted peers
- Community services
Improves our defensive controls

- Indicators to block/detect
- Higher-leverage TTPs
- Prioritize events and alarms
- Context for incident review
Empowers other security teams

- Security policy changes
- Malcode samples to acquire
- Vulnerabilities to pen test
- Indicators for forensic scans
Informs strategic decisions

- Security architecture changes
- IT investment decisions
- Supplier due diligence
- Trends in business risk
Get Trending Threat Insights Delivered to Your Inbox With Our Free Cyber Daily

http://go.recordedfuture.com/cyber-daily
There Can Be Only One!: Last CTI Vendor Standing Pitch

Jess Parnell, Centripetal Networks
Layered Active Blocking & Logging

• Start with country blocking

  • Inbound drop/no log
  • Outbound resets/log

• OFAC is the easiest place to start

• ITAR & others unfriendly to US Law Enforcement
Pyramid of IOCs

- IP: 50.117.38[.]170
- IP hosts many sites
- Domain: opm-learning[.]org
- URL: opm-learning[.]org/badfile.exe

Ref: https://www.passivetotal.org/passive/opm-learning.org
Ref: https://www.threatconnect.com/opm-breach-analysis/
Actively Block on New Threats Discovered

- RuleGate® plugin updates IOCs from FireEye NX series malware sandbox
- Policies configured to actively block newly discovered IOCs
Send to SIEM: Correlate End-User

- RuleGate® sends events to the SIEM with applied threat intelligence context in real-time
Why not use my Firewall?

- GEO blocking China
  - ~ 300 Million IPs
  - ~ 8K RuleGate Rules
- GEO blocking in NGFW
- Increased Latency
- RuleGate Performance
  - 5M+ Indicators/Rules
  - Up to 20Gbps aggregate throughput
  - < 10µS Latency

RuleGate handles 125x more indicators than the most powerful Next-Generation Firewall (NGFW) available.
Why not use my SIEM?

- NO Active Blocking Capability
- Avg Security Team has 1-3M Indicators
- Not feasible within current SIEM
- List-based matching difficult to manage
- ~28K Breaks SIEM

SIEM is purely for analysis, and has no Active Blocking capability
Is the RuleGate a Threat Intelligence Platform (TIP)?

- NO it’s Threat Enforcement
- In-line deployment for Active Blocking
Indicators from Partners you Trust

- Open Intelligence Platform
- Open Source & Commercial
- Fully Integrated: Automatic Updates & Application
- Source Multi-Attribution
- Technology Integrations
  - Malware Detection
  - Threat Intelligence Platforms
  - SIEM Tools

(not an exhaustive list of Centripetal intelligence sources)
You will NOT be overwhelmed with Actionable Intelligence

• Pivot to Source
• Targeted Packet Capture
• Instant Data Correlation
• Enterprise Specific Risk Models
• Geographic Visualizations

QuickThreat® - Pivot to Source
Thank You
There Can Be Only One!: Last CTI Vendor Standing Pitch

Roselle Safran, UpLevel Security
What is Uplevel?
Intelligence-based Incident Response Platform
Incident Response Lifecycle Needs CTI at Every Stage

Mitigation/Remediation

Triage

Investigation

More effective with CTI

More accurate with CTI

More efficient with CTI
Why is Uplevel Awesome?

Top 5 Reasons
Reason #5:  
Uplevel is Built By Practitioners For Practitioners

Cybersecurity Operational Expertise

Cybersecurity Data Analysis Expertise
Reason #4: Uplevel Integrates Incident Management and Threat Intel Management into One System

- Collaborative
- Comprehensive
- Consistent
Reason #3: Uplevel Preserves Context

- Sources
- Relationships
- Confidence Levels
Reason #2:
Uplevel Provides Graph Intelligence
Reason #1: Uplevel Automates Tasks So Analysts Can Focus on the Interesting and Challenging Work

- Workflow orchestration
  - Integrations with a variety of tools
  - Enterprise-specific processes
- Data enrichment
  - Threat intelligence feeds
  - Open source information