

Scale Threat Response, From One to Thousands

Unmask adversary-threat infrastructure, anywhere on-demand

Cybercriminals, hacktivists, and nation-state threats all evolve tactics, techniques, and procedures (TTPs) to improve their malicious capabilities. However, adversary behaviors change continuously—malware variants, distribution and alliances, zeroday leaks, and tooling. These ongoing changes prevent longlasting protection that can scale to cover the enterprise's digital footprint.

Sustainable, scalable cyber defense comes from fingerprinting adversary-threat infrastructure and observing malicious systems relevant to the enterprise's digital attack surface.

Whether threat infrastructure is associated with one threat actor or used by thousands of adversaries (e.g., kits, C2, leaked tools), security teams require high-fidelity security intelligence to find and eliminate threats with confidence.

Highlights | RiskIQ Illuminate®

- 10+ years of digital history and tracking the global attack surface.
- Dynamic risk and reputation scoring based on real-world observations.
- Multi-factor threat fingerprinting via crawling, registry, history, and OSINT.
- Automate downstream playbooks with easy reputation APIs and on-demand threat observations..
- Elastic defense for continuous change: external threats and your attack surface.

SCENARIO: From One to Many

Active and historical, real-world observations

Simply gathering intelligence from open sources or network telemetry and antimalware is not enough to solve the current security challenge to unravel what is you from what is another, what's good from what's malicious, and adversaries from allies. Relevant, actionable intelligence lets you personalize real and vital threats to you.

With the rise of remote workforces, digital supply chains, and global networks, the time could not be more advantageous for threat actors to create and distribute remote access trojan (RAT) malware.

Digital growth and change have allowed RATs to proliferate while hiding in plain sight.

Q 185.1	83.98.182		Search Options			×		
 PassiveT 18 First Seen Last Seen Country 	otal Intelligend 5.183.98 - - NL	3.182 Detail NetBlock ASN Organization	185.183.98 0/24 A560117 - 45 Host Seilor 1d	OS Hosting Provider	Reputatic Data & Ke Insights	on ≩y		
 Reputat Severity <!--</th--><th>Rule RisklQ Intel Art ASN SSL certificate Country</th><th>ious (Score: 100 c icle C self-signed S ir</th><th>b) escription bibliqueRAT returns with new of ifrastructure hosted by this AS elf-signed certificates may inc ifrastructure hosted in this co</th><th>ked websites be malicious vior to be malicious</th><th></th>	Rule RisklQ Intel Art ASN SSL certificate Country	ious (Score: 100 c icle C self-signed S ir	b) escription bibliqueRAT returns with new of ifrastructure hosted by this AS elf-signed certificates may inc ifrastructure hosted in this co	ked websites be malicious vior to be malicious				

https://community.riskiq.com/research?query=185.183.98.182

THREAT: ObliqueRAT

Fingerprint Adversaries, Digital Trace Analysis

You discover a machine infected with a redesigned malicious remote access trojan (RAT) named ObliqueRAT, likely related to a new campaign cited by Talos. However, the new RAT variant is delivered via adversary-controlled websites.

These websites, created for RAT development and distribution, are packed with privacy controls and have no known history on the internet. <u>Cisco Talso published</u> four indicators, one IP address, and three domains:

- 185[.]183.98.182
- Larsentobro[.]com
- Micrsoft[.]ddns.net
- yepp[.]ddns.net

INVESTIGATE: Remote Access Trojan (ObliqueRAT)

Dynamic reputation scoring for rapid triage and impact analysis

Quickly determine paths of investigation via dynamic reputation scoring and priorities based on the global attack surface.

ObliqueRAT was reported to be associated with the IP address 185[.]183.98.182 (seen above).

Search the IP address to see the most current reputation. The reputation for the IP address related to ObliqueRAT, 185[.]183.98.182, results as *Malicious* with high confidence of 100.

The malicious IP address had privacy controls concealing information from registries, such as WHOIS. However, the malicious IP shows relationships to other threat indicators found in open-source intelligence (OSINT), including systemgenerated certificates and host country.

Insights

Privacy controls prevent tracking IP address details via registries (e.g., WHOIS).

RAT malware is a widely distributed threat utility, nearly certain to be found within other IP addresses and domains.

Common names and systemgenerated SSL certificates are effective sub-IP threat indicators.

Actions

Leverage reputation scoring based on identifiers below the IP-layer, such as SSL certificates and history.

Track and trace malicious infrastructure changes, capabilities, and activity.

Extract related infrastructure and digital fingerprints embedded in internet telemetry.

Apply expanded threat intelligence to global defenses.

Automate downstream playbooks and workflows for elastic protection coverage from a single threat actor to thousands. Observations showed IP address 185[.]183.98.182 running Windows Remote Desktop Service along with a systemgenerated certificate containing the hostname WIN-BL01IL47JMV.

The hostname was then found to be related to dozens of malicious IP addresses and hundreds of domains. Enterprise security teams can uncover adversary-threat infrastructure for high-impact investigations and response from a single alert and indicator.

AUTOMATE: Threat Indicators, Protection

Examining the SSL Certificate History on the IP address, we can see two different several self-signed certificates and two unique hostnames WIN-BLO1IL47JMV and WIN-UNIEC1PV56D, demonstrating an infrastructure overlap and a lead to new related indicators.



Key Insights Issue Date & Hostname

RELEVANCE: Attack Surface Intelligence

Active and historical discovery for complete visibility

Attack surface intelligence identifies and distinguishes resources and digital systems across the open and closed web

Security intelligence that combines attack surface insights with real-world observations of RAT malware enables a more impactful response.



https://community.riskiq.com/search/185.183.98.182/ certificates

*Security Impact Score based on required cybersecurity expertise, investigation time, and scope of protection attained.

Results

Starting with a single IP address from an open-source article, uncovered:

- Adversary infrastructure, RDP
- SSL certificate-based identifiers
- 100+ additional IP addresses
- 1,000+ additional domains
- Continuously updated controls

SECURITY

89*

https://community.riskiq.com/search/185.183.98.182/services

	Q WIN-BL01IL47JMV			Illuminate 🛠 😌 🚨
WIN-BL01IL47JM	(subjectCommonName)			
ertificate Search				
* DATA				
Filters 0	SSI Cartificate Search			Download Conv
SHA-1 (78 / 78)		05 (0		
✓ × 0±05377411bb 1	1 - 25 01 / 6 V Sort : Last Seen Descending V	∠o/raye ∨	Last Seen	Infrastructure
✓ ≍ 0d75010d94e6 1	 0d75010d94e64c79b6b2c9ca39a811859e458883 	2021-04-18	2021-04-20	185.183.98.182
✓ ※ 0eb6d7dda3d2e 1	Serial Number 72114743680111752544206752509530752086			
✓ × 165d92e2c7c8b 1	Issued 2021-04-16			
w More	Expires 2021-10-16			
EIDST SEEN (52/79)	Common Name VAN-REOTE 47 IMV (whiler)			
FIRST BEEN (52776)	WIN-BLOTIL47JMV (subject)			
× × 2020-00-03 15				
× × 2020-09-14 3	Alternative Names			
× × 2020-09-02 3	Organization Name			
✓ × 2020-08-07 2	SSL Version 3			
how More	Organization Unit			
LAST SEEN (57 / 78)	Street Address			
✓ × 2020-09-27 6	Locality			
√ × 2021-04-20 6	State/Province			
√ × 2020-10-31 3	Saleriovice			
√ % 2020-06-10 2	Country			
√ × 2020-06-12 2	70ce9a7bdf90076ae1260df085c8c97228bfe03a	2021-03-19	2021-04-20	185.45.193.23
how More		2021-03-22	2021-04-20	
UNIQUE IP (47 / 103)	1b9651020241506f2f4964dd39dde7209cfcea49	101-03-22	101.004.20	185.117.73.195
✓ ≍ 185.183.98.182 6	55e73458cfd12cd6c7f237960dec8c3c3005d4e1	2021-04-02	2021-04-20	185.45.193.60
√ % 185.117.73.195 5	 E053-14544-308	2021-03-04	2021-04-20	
√ ≍ 185.82.202.154 5	 b953e11500e306ccebe2c7436986400015518095 			100.40.103./
✓ × 185.183.98.162 4	f2133b4bd2ce226c31e9dae65a50985aba7a2785	2021-01-22	2021-04-20	185.82 202 145

78 IP addresses are linked to hostname WIN-BL01IL47JMV. Each IP address will lead to additional hostnames and new IP addresses

VISIBILITY: Finding New Related Infrastructure

Each Pivot in the self-signed certificate common name issuer hostname leads to new IP addresses. Each new IP address leads to new related self-signed certificates with new unique hostnames contained in the common name issuer.

https://community.riskig.com	n/search/certificate	e/subjectCommonName/	WIN-BL011L47JM

E ORISKIQ	Q WIN-UNIEC1PV56D			Illuminate 🛠 🕀 🊨
🕒 WIN-UNIEC1PV56D (SubjectCommonNamol			
Certificate Search	✓ 1 - 25 of 100 × ► Sort : Last Seen Descending	g ∽ 25 / Page ∽		
* DATA	•			
Elter O	551 Cariffrais Search 0			
711A 1 10001000	1 - 25 of 100 × Sort : Last Seen Descending × 25 / Page ×			Download Copy
x X 01/109067169r 1	544.4	Einst Soon	Last Source	Infrastructure.
✓ X 02dfe4e8c7d3fc 1		2021-02-01	2021-04-20	
✓ X 075c0b5/69aa1 1	eso2ecasdeoads/6000500400164600660008			185.45.193.29
✓ × 099a5071835d 1	396642022//166308/669560313/422522143			
✓ × 0a0000d10e8a 1	Issued 2021-01-31			
Show More	Expires 2021-08-02			
FIRST SEEN (62/100)	Common Name WIN-UNIEC1PV56D (subject)			
✓ X 2019-06-23 12	WIN-UNIEC1PV56D (Issuer)			
√ × 2019-12-26 5	Alternative Names			
√ × 2019-11-21 4	Organization Name			
√ × 2019-09-16 3	SSI Version 3			
√ × 2019-10-09 3	Overselection 1 lat			
Show More	organization onit			
LAST SEEN (65/100)	Street Address			
✓ × 2020-01-24 6	Locality			
✓ X 2019-10-04 4	State/Province			
√ x 2019-10-13 4	Country			
✓ x 2019-10-30 3		2020-06-17	2020-11-14	
Show More	e880f7ae696b1d469fa8f1f0b41f196cb8aa34fa	1010-00-17	2020-11-14	185.82.202.162
UNIQUE IP (73/111)	c4d39c9ec5e54ed605990918d25dba0ac611e97a	2020-05-18	2020-10-14	185.82.202.159
✓ × 185.45.193.16 4	#70e77549a2cc81905dfb4ed12dd8a954a38070	2020-03-24	2020-08-22	185.183.98.166
√ % 185.82.202.132 4	6e76d3dcdf1987743814285ec5c0fc85d02c995b	2020-03-30	2020-07-03	185.183.98.176
√ % 185.82.202.143 4				
√ × 185.82.202.159 4	02dfa4e8c7d3fc960f4ace08e635eceb24cf67e5	2020-04-03	2020-06-06	185.82.202.151
✓ ※ 185.117.73.219 3		2020 02 04	2020.05.02	

100 IP addresses are linked to hostname WIN-UNIEC1PV56D. Each IP address will lead to additional hostnames and new IP addresses

https://community.riskiq.com/search/certificate/subjectCommonName/WIN-UNIEC1PV56D

SCENARIO: From One to Many

Scaling Threat Investigations

Speed and repeatability are key to investigations. Many Cyber Threat Investigators utilize scripts and API to perform multiple tasks in series to get accurate, repeatable results.

AUTOMATE: Threat Indicators, Protection

By understanding the manual process of this investigation script can automate the investigation.

Steps:

- 1. Start with IP address
- 2. Find all self-signed Certificate
- 3. Search on the common name issuer hostnames
- 4. Find all IP addresses associated with common name issuer.
- 5. Repeat until no new unique IP address or Common Name issuer hostnames appear.
- 6. Then determine the reputation score for each unique IP address and unique domain.



		neputation								
In [18]:	imp	import pandas as pd								
	def	<pre>def build_rep_list():</pre>								
		<pre>for rep in reputation_history_from_ips:</pre>								
	yield {									
		'so	ore':	rep.get('						
		'c]	Lassif	ication':						
	df	<pre>} = pd.DataFra </pre>	ame(bu	ild rep li:						
	df.	sort_values	(by <mark>=</mark> "s	core", asc						
Out[18]:										
	_	ip	score	classification						
	0	185.82.202.132	100	MALICIOUS						
	26	185.45.193.7	100	MALICIOUS						
	42	185.45.193.61	100	MALICIOUS						
	52	185.183.98.182	100	MALICIOUS						
	59	185.82.202.131	74	SUSPICIOUS						
	68	185.82.202.173	74	SUSPICIOUS						
	67	185.183.98.163	74	SUSPICIOUS						
	66	185.45.193.24	74	SUSPICIOUS						
	64	185.82.202.141	74	SUSPICIOUS						
	63	185.117.73.213	74	SUSPICIOUS						
	62	185.45.193.50	74	SUSPICIOUS						
		105 15 100 07		0.100101010						

18 Reputation Score for IP addresses formatted

	19. Reputation score for domains formatted							
In [28]:	<pre>import pandas as pd pd.set_option('display.max_rows', None) def build_rep_domain_list(): for rep in reputation_history_from_domains: yield { 'domain': rep['query'],</pre>							
	df = p df.son	<pre>od.DataFrame(build_rep_domain_list()) ct_values(by="score", ascending=False</pre>)					
	83	wrp7rts.vi0lowd.top	72	SUSPICIOUS				
	205	lisk.movecrypto.online	72	SUSPICIOUS				
	1264	o6qh.v08ca.top	72	SUSPICIOUS				
	1932	zbzx6.z0zenbw.top	72	SUSPICIOUS				
	1933	ex4tomq4.cc	72	SUSPICIOUS				
	813	nexia.flycrucialsknow.xyz	72	SUSPICIOUS				
	202	ftzp2p.k4b8h.top	72	SUSPICIOUS				
	1199	x05h8.xoka7g1.top	72	SUSPICIOUS				
	91	quest.basesizens.xyz	72	SUSPICIOUS				
	107	ebru4.tjgwmzn.top	72	SUSPICIOUS				
	1160	jnorb.ce3uuyr.top	72	SUSPICIOUS				
	72	SUSPICIOUS						
131 djhdooudhdghauykfg.ex4tomq4.cc 72 SL								
		aunat arastusaash uur	70					

Over 90 Unique IP addresses were discovered all had a dynamic reputation score of Malicious or Suspicious

After just 3 degrees of separation from the initial IP address, these hostnames were found in self-signed certificates:

WIN-BL01IL47JMV WIN-UNIEC1PV56D WIN-BVLRV1JQS28 WIN-U2QBNCSEVVG WIN-MJPCIGVK17I WIN-BJ8C2GA1PMK WIN-host2000-95 WIN-FKLITKTLLT2 WIN-FKLITKTLLT2 WIN-FKLITKTLLT2 WIN-VL36D5H5VCA WIN-09C3GCCMMI WIN-0VAE1841EL4 WIN-UNIEC1PV56E

Over 1900 Unique domains were discovered over 576 had a dynamic reputation score of Malicious or Suspicious

Scripts can be run any time to find new upto-date indicators that can be used in your organization's SIEM to SOAR, EDR to MSSP.

RiskIQ Illuminate SecOps Intelligence— API Based Module

RiskIQ's SecOps Intelligence module provides unique insights and security information suited for easy integration with SIEMs and other security unified management platforms. Security professionals using SecOps Intelligence integrated into their single pane of glass system use RiskIQ reputation information to distinguish friend from foe and identify items to be escalated for further investigation.

Users have access to RiskIQ Intelligence & Reputation Data as easy-to-integrate feeds and simple APIs for use in SIEMs and other security management solutions. RiskIQ leverages our research-assisted artificial intelligence and machine learning profiling to frequently updated feeds and markers for reputation scores to deliver actionable intelligence at scale.

The use of this module significantly boosts the accuracy of a team's event review and reduces the time to either dismiss or escalate these events by leveraging our reputation scoring data. Users also have access to our PassiveTotal community platform, enabling teams to quickly pivot through 10+ years of historical data for additional investigation. The SecOps Intelligence module enables teams running day-to-day security operations, including Operations Center and Detection & Response teams, to easily access the most up-to-date security information in the industry. It assists analysts in making fast and efficient decisions when reviewing security events.

API-Based Integrations:

The SecOps Intelligence module also provides a single API to streamline an organization's efforts across multiple platforms. RiskIQ provides a reputation score via the easily integrated API to reveal insights, including relationships to known exploits or hacker activity.

Furthermore, SecOps Intelligence users will have access to RiskIQ's Splunk application that supports our reputation data.

Organizations can use this alerting feature to proactively block malicious infrastructure within their environments, providing better situational awareness and reducing possible exposure to future attacks.

Key Features

- Enrichment feeds via Amazon S3 bucket
- Newly observed domains act as a layer of protection
- Newly observed hosts act as an added layer of protection against quick attack campaigns
- Malware and phishing with feed-based information
- Reputation data and key insights with rating and key contributing factors
- Easily integrated API based entity reputation score lookups

Example Illuminate API Request

https://api.passivetotal.org/index.html

JSON Request Curl Example		_
{ "query": "passiveto }	otal.org"	
Response		
<pre>{ "subdomains": [], "sinkhole": false, "tld": ".org", "primaryDomain": "p. "queryValue": "pass "queryType": "domail "everCompromised": " "tag_meta": { "mytag": { "created_at } }, "classification": " "tags": ["mytag"], "dynamicDns": false } Send a Sample Request</pre>	assivetotal.org", sivetotal.org", .n", false, "johan@riskiq.net", ": "2017-03-30T01:05:12.629000" 'non_malicious",	
	https://api.passivetotal.org/v2/enrichment ur	Ge
B		Fo

Key Benefits

- No new process changes or context switching, just enhanced capabilities
- No new tools, easily integrated
- Save analysts unnecessary work and scale their techniques
- Research is saved and correlated
- Turn a one-time hunt into a detection capability
- Respond proactively with precision-targeted detection logic

Get Enrichment Data For A Query

Python wrapper for RiskIQ PassiveTotal API

https://pypi.org/project/passivetotal/

https://passivetotal.readthedocs.io/en/latest/

Vendor-agnostic flexible APIs and apps, and co-development with Interlock Partners

A web interface option with API access available to companies and their support teams is extremely handy when investigating detected events. In-app mitigation workflow, along with continuous monitoring of online resources, lets companies quickly take action, know when threats have been successfully remediated, and track event lifecycle metrics to report on threat response efficiency.

splunk>	enterprise	App: RiskiQ PassiveTotal App	o For Spl 🔻			🚯 brandon 🔻	Messages 🔻	Settings 🔻	Activity -	Help 🔻	Find Q.
Live Inve	stigation Loca	I Investigation Search Hi	istory Search	Contact Us 12	Request an Enterp	rise Setup 🛽				Ô	RISKIQ
Live I Enter an riskiq.c	Live Investigation Edit Export • Enter an IP or Domain Name View in PassiveTotal riskiq.com Hide Fitters										
Resc	Resolutions (16) Whols (6) Certificates (100) Subdomains (3K) Trackers (773) Components (8K) Host Pairs (10K) OSINT (10) Hashes (1) DNS (20) Matching Events (203) Records Emails Registrars Name Servers Phone Numbers Organization										
WHOIS	RECORDS				Raw Rec	ord \$					
i	Change Date 🗘				Domain M	ame: RISKIQ.COM					
~	2017-01-05				Regis	try Domain ID: 31 trar WHOIS Server	4061295_DOMAI : whois.godad	N_COM-VRSN dy.com			
	Attribute 🗘	Value ‡	Regis	Registrar URL: http://www.godaddy.com Updated Date: 2017-01-05719:22:517							
	Updated On	2017-01-05	Creat	Creation Date: 2006-01-12T19:33:26Z							
	Created On	2006-01-12			Regis	try Expiry Date: trar: GoDaddy.com	2026-01-12119 , LLC	:33:262			
	Expires At	2026-01-12			Regis	Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: 480-624-2595					
	WHOIS Server	whois.godaddy.com			Regis						
Registran GoDaddy.com, LLC Domain Status: clientDeleteProhibited https://icann.c Domain Status: clientRenewProhibited https://icann.c							cann.org/epp# ann.org/epp#	<pre>#clientDele clientRenew</pre>	eteProhibited wProhibited		
	Email	abuse@godaddy.com (regi	strant)		Doma	n Status: client⊺	ransferProhib	ited	2.11		

Splunk Integrations with Illuminate API

Integrations Key Benefits

- Automatically triage every indicator found within your Splunk logs to drive alert creation and further Internet enrichment using RiskIQ Illuminate SecOps Module.
- Enhance the security ecosystem—people, processes, and technologies
- Maximize investments and enable attack surface awareness throughout the security stack
- Future-proof digital risk and threat programs with intelligent systems, technologies, and partnerships



RisklQ, Inc.

22 Battery Street, 10th Floor San Francisco, CA. 94111

≤ sales@riskiq.net

L 1888.415.4447

Learn more at riskiq.com

Copyright © 2021 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 05_21