

# Identifier Systems Investigation Template

<b>Investigator</b>		
<b>Investigator Contact email:</b>		
<b>Investigator Contact phone:</b>		
<b>Investigation Name</b>		
<b>Investigation Number</b>		
<b>Creation Date:</b>		
<b>Last updated:</b>		
<b>Domain(s) of Interest:</b>		
<a href="#">Link to file of domains</a>		
<b>Associated URLs of Interest:</b>		
<a href="#">Link to file of URLs</a>		
<b>Domain/hostname found in:</b>	X	
		Email header
		Email message body
		Web page
		Text/SMS
		QR code
		Comment or forum spam
		File repository
		Cloud or developer account
		WordPress account
		Free web hosting (subdomain) provider
		Other:

## Identifier Systems Investigation Template

Domain Abuse/Cybercrime	X	
		Email or messaging spam
		Comment or forum spam
		Scam site
		Counterfeit goods site
		Illegal pharma site
		Botnet Controller/DGA domain
		Defacement page
		Phish email
		Phishing page
		Other:
Malware ( <a href="#">classification</a> )	X	
		IoT Malware
	IoT Bot	Malware Name:
		Endpoint Malware
	Backdoor/RAT	Malware Name:
	Crypto Malware	Malware Name:
	Dropper/Loader	Malware Name:
	Infostealer	Malware Name:
	Malicious Document	Document Type:
	Malicious Executable	Executable Type:
	Ransomware	Ransomware Name:
		Malicious IP Address
	Traffic Injector	Injector Type:
	Attack Ware	Type:

# Identifier Systems Investigation Template

Name Server Information		
Name server names:		
		<a href="#">Link to file of NS names</a>
Name server addresses (glue)		
		<a href="#">Link to file of NS glue</a>
Interesting DNS Zone data:		<a href="#">Link to dig or nslookup output</a>
SOA email address:		
SOA TTL:		
MX resource records:		
TXT resource records:		
Address resource records:		
CNAME resource records:		
Other resource records of interest		

# Identifier Systems Investigation Template

Domain Registration Whois/RDAP	
	<a href="#">Link to Whois records</a>
Creation Date:	
Updated Date:	
Registry Expiry Date:	
Sponsoring Registrar:	
Sponsoring Registrar IANA ID:	
WHOIS Server:	
Domain Status:	
Registrant ID:	
Registrant Name:	
Registrant Organization:	
Registrant Postal Address:	
Registrant Phone:	
Registrant Fax:	
Admin ID:	
Admin Name:	
Admin Organization:	
Admin Postal Address:	
Admin Phone:	
Admin Fax:	
Tech ID:	
Tech Name:	
Tech Organization:	
Tech Postal Address	
Tech Phone:	
Tech Fax:	

# Identifier Systems Investigation Template

IP and ASN Whois	
Network Whois/RDAP	RESTful links
Net Range	
CIDR	
Name	
Handle	
Parent	
Net Type	
Origin AS	
Organization	
Registration Date	
Last Updated	
Name	
Handle	
Address	
Registration Date	
Last Updated	
Technical Contact	
Name	
Handle	
Company	
Address	
Registration Date	
Last Updated	
Phone	
Email	
Abuse Contact	
Name	
Handle	
Company	
Address	
Registration Date	
Last Updated	
Phone	
Email	

## Identifier Systems Investigation Template

REPUTATION		
Domain name/URLs:	X	
		Spamhaus DBL <a href="http://www.spamhaus.org/dbl/">http://www.spamhaus.org/dbl/</a>
		Spamhaus BCL <a href="http://www.spamhaus.org/bcl/">http://www.spamhaus.org/bcl/</a>
		APWG eCrime eXchange <a href="https://www.ecrimex.net/">https://www.ecrimex.net/</a>
		OpenPhish <a href="http://www.openphish.com/">http://www.openphish.com/</a>
		Abuse.ch <a href="https://abuse.ch">https://abuse.ch</a>
		ZeuS Tracker <a href="https://zeustracker.abuse.ch/blocklist.php">https://zeustracker.abuse.ch/blocklist.php</a>
		SURBL <a href="http://www.surbl.org/lists">http://www.surbl.org/lists</a>
		Invalument <a href="https://www.invalument.com/">https://www.invalument.com/</a>
		PhishTank <a href="http://phishtank.org/">http://phishtank.org/</a>
		DomainIQ <a href="https://www.domainiq.dev/">https://www.domainiq.dev/</a>
		Other:
IP network, ASN, Hosting	X	Links to RBL data
		Spamhaus SBL <a href="http://www.spamhaus.org/sbl/">http://www.spamhaus.org/sbl/</a>
		Malware Patrol <a href="https://www.malwarepatrol.net/">https://www.malwarepatrol.net/</a>
		URLhaus <a href="https://urlhaus.abuse.ch">https://urlhaus.abuse.ch</a>
		MalwareURL <a href="https://malwareurl.com">https://malwareurl.com</a>
		Domain Tools <a href="https://domaintools.com">https://domaintools.com</a>
		Zetalytics passive DNS <a href="https://zetalytics.com/">https://zetalytics.com/</a>
MX records	X	
		SenderScore <a href="https://senderscore.org/">https://senderscore.org/</a>
		Sender Base <a href="http://www.senderbase.org/">http://www.senderbase.org/</a>
		Mxtoolbox <a href="http://mxtoolbox.com/blacklists.aspx">http://mxtoolbox.com/blacklists.aspx</a>
		Other:
Malware	X	
		VirusTotal <a href="http://www.virustotal.com/">http://www.virustotal.com/</a>
		ANY.RUN <a href="https://any.run">https://any.run</a>
		Seclytics <a href="https://seclytics.com">https://seclytics.com</a>
		Malware Tracker <a href="https://www.malwaretracker.com/">https://www.malwaretracker.com/</a>
		Other:

# Identifier Systems Investigation Template

## NOTES