

M&A, Forgotten Son of Information Security

Dr. Marco Ermini, CISA CISM
2017 Telefónica Germany

Agenda

- » Why M&A need Cyber Security support?
- » Aren't they just ordinary business transactions?
- » They seem to occur nearly every day, so what is so special about them that they require special security support, or any security support at all?
- » What value does a security professional bring to the team?



The Academic Minute...

- » Black's Law Dictionary defines mergers and acquisitions as the following:
 - Merger: The union of two or more corporations by the transfer of property of all, to one of them, which continues in existence, the others being swallowed up or merged therein...
 - Acquisition: The act of becoming the owner of a certain property...
 - Divestiture: to deprive; to take away; to withdraw



The Academic Minute...

- » Acquisition of Total Assets
 - Liquidate
 - Break up and sell
 - Integrate
- » Acquisition
- » Merger
- » Divestiture



The Academic Minute...

- » It is all about...
 1. Costs Control,
 2. Market Share,
 3. Regulatory Landscape
 4. Others...



Business Drivers

- » Confidentiality
- » Speed
- » Business as usual
 - Zero Impact
- » Informed Business Decision on Risk



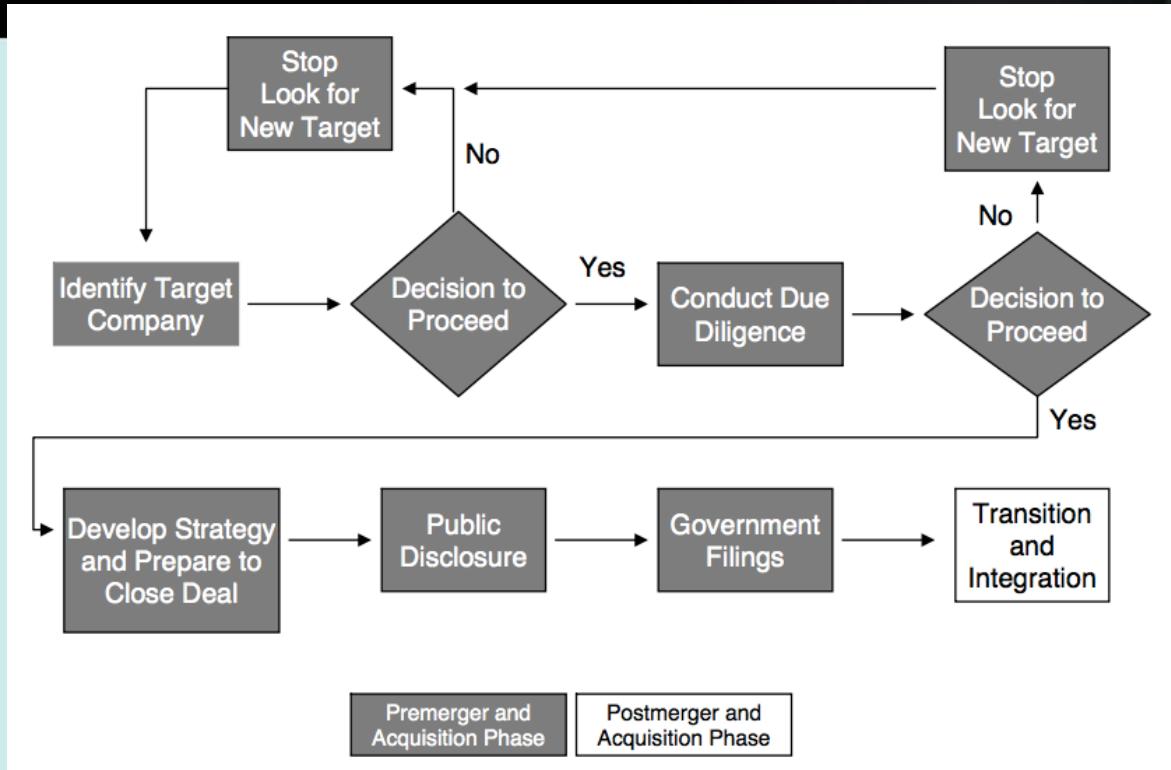
Why M&A Fail?

- » The acquiring company does not properly assess the value of the target company
- » Inability of the acquiring company to successfully integrate the target company that leads to a failed acquisition

"It is well known in the M&A community that most acquisitions fail to create shareholder value, that is, they end up as a negative sum after paying acquisition premium and banker fees, impossible to get synergies to make up loss. The acquisitions that do create value are either a version of corporate venture capital (large company scooping tiny team), or mid-cap industrials buying a supplier. Few and far between..."



Typical M&A Diagram Flow



Premerger and
Acquisition Phase

Postmerger and
Acquisition Phase



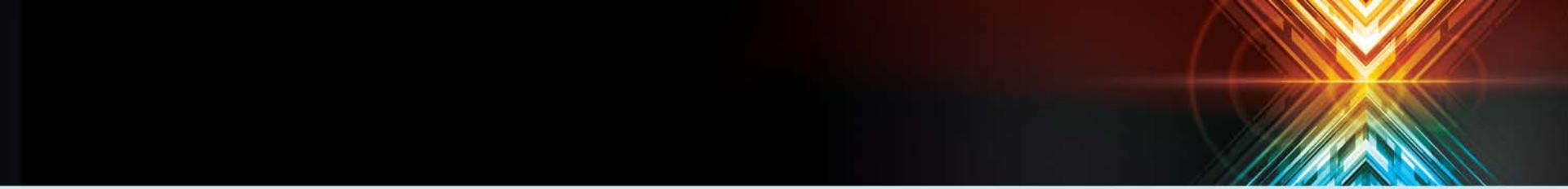
The Four “C”s



The Four Cs

- » Capture
- » Connect
- » Combine
- » Consolidate





Threats and Response



Scoping the Threats

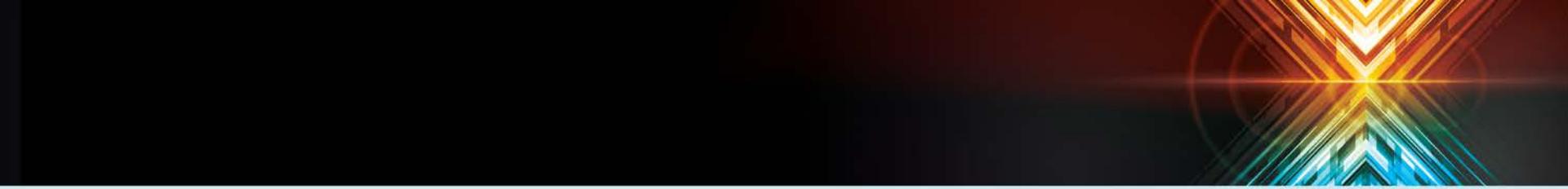
- » Special Interest Groups – gain from the Operation
 - Financial Criminals
 - Competitors
 - Acquisition / Merger Company
 - Disgruntled Employees
- » General Interest Groups – gain from Impact
 - Script Kiddies / Hackers
 - Hacktivists / Terrorists
 - Spies



Scoping the Risks

- » Publicity, raising profile — your interest gets attacker's interest!
- » Impact on:
 - Resources
 - Technologies
 - Infrastructure
- » Disgruntled Employees
- » Change in threat and risk model
- » Absorbing unknown / Confusion
- » Creating new attack vectors and window of opportunity
- » Business drivers can force this the Security Manager very quickly
- » **Are we all really equipped for change?**





The Security Manager



The Role of a Security Manager

- » Protecting the effort itself
 - Confidentiality of the total effort
 - Confidentiality of the team's work
- » Evaluating the security condition of the target company
 - Impact on the deal's value
 - Asking the right questions
- » Providing subject matter expertise
 - Identify Security Requirements for the New Company
 - Controlling Rumors
 - Managing Global/International Aspects
 - “Team Consultant”
 - Low Hanging Fruits



Importance of Confidentiality

- » Premature Disclosure of Intent
 - Loss of key employees
 - Bidding wars
 - SEC Liability
 - Loss of Initiative
 - Loss of Goodwill
 - Target Company
 - 3rd Parties relationships
 - Customer relationships



Protecting the operation

- » Unintended Release
- » Unauthorized Release
- » Protection from competitive intelligence efforts
- » Documents Control



The Security Manager in action

- » Preliminary background investigations
 - Collection of Open-Source information
- » Due diligence
 - More in-depth look
 - Estimation of Costs of Cyber Security
- » Operations security
 - Protect operational activities
 - Develop and implement protective measures
 - Appropriate for each phase of the acquisition





Preliminary Work



How can I verify an M&A Target candidate?

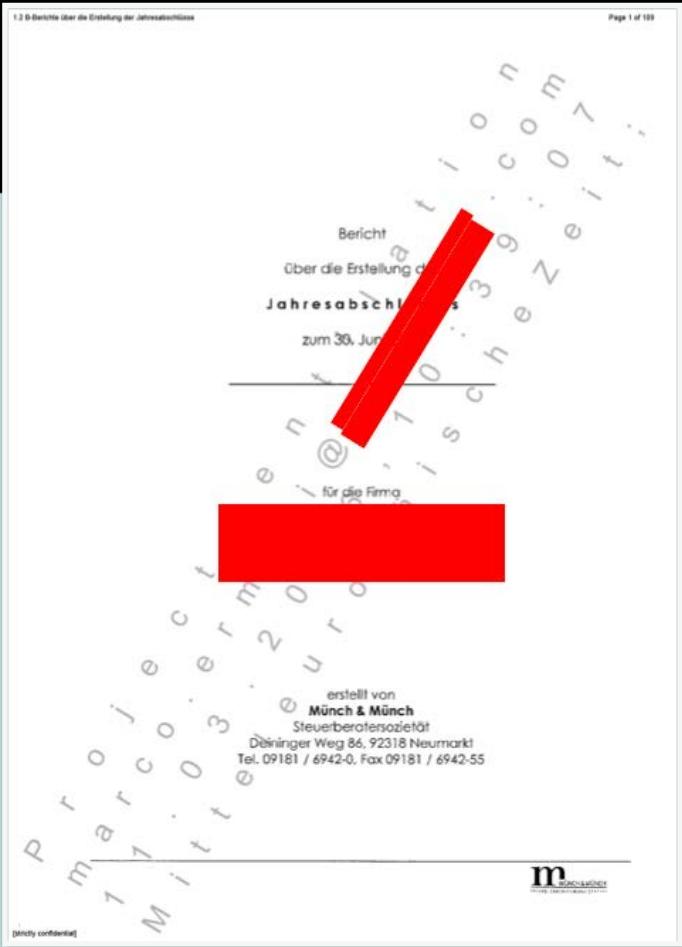
- » You cannot *explicitly* test your acquisition's candidate
- » You cannot simply ask them for their vulnerability assessments' results
- » Not all companies have a structured and mature security program
- » You cannot silently test them either



External Sources

- » Professional Associations
- » Service Providers
- » Public (Open) Sources
- » Job Applications/Job Postings





Entwicklung des Anlagevermögens nach Steuergesetz vom 01.07.2014 bis 30.06.2015

Konto Inventar	Bezeichnung Inventarbezeichnung	Datum ATA-Art S-Nr. S-S.	Entw. der 01.07.2014 Euro	Stand zum 30.06.2015 Euro	Zugang Abgang Tum	Umbuchung Euro	Abschreibung Euro	Zuschreibung Euro	Stand zum 30.06.2015 Euro
670 Geringwertige Wirtschaftsgüter									
Übertrag									
	Ansch./Herst. €		347.642,54						0,00
	Abschreibung		347.642,54						0,00
			347.642,54						0,00
	Buchwerte	0,00	347.642,54						0,00
670257 Zugänge GWG 01/15		31.01.2015 AHK							0,00
	GWG/noll Abschr.		-40.555,00						0,00
		01/00 / 100,00 BW	0,00	5,00			40.555,00	0,00	
670259 Kon.Megro, Untersuchungs- seige		29.01.2015 AHK		193,32					0,00
	GWG/noll Abschr.		-193,32						0,00
		01/00 / 100,00 BW	0,00	193,32			193,32	0,00	
670260 Notebooksbilliger.de, hof ebook Lenovo 850-40		04.03.2015 AHK							0,00
	GWG/noll Abschr.		-361,44						0,00
		01/00 / 100,00 BW	0,00	361,44			361,44	0,00	
670261 Nux 30x MS Office Home and Business 2013		06.02.2015 AHK		5.550,00					0,00
	GWG/noll Abschr.		-5.550,00						0,00
		01/00 / 100,00 BW	0,00	5.550,00			5.550,00	0,00	
670262 Nux 10x Microsoft Office Standart 2013		06.02.2015 AHK		3.780,00					0,00
	GWG/noll Abschr.		-3.780,00						0,00
		01/00 / 100,00 BW	0,00	3.780,00			3.780,00	0,00	
670263 Lotter ident, Zweck 0409 kostiger@		04.03.2015 AHK		369,30					0,00
	GWG/noll Abschr.		-369,30						0,00
		01/00 / 100,00 BW	0,00	369,30			369,30	0,00	
670264 Würth, Werkzeughöffl		05.03.2015 AHK		188,60					0,00
	GWG/noll Abschr.		-188,60						0,00
		01/00 / 100,00 BW	0,00	188,60			188,60	0,00	
Übertrag									0,00
	Ansch./Herst.-€		398.640,40						0,00
	Abschreibung		-398.640,40						0,00
			398.640,40						0,00
	Buchwerte	0,00	398.640,40						0,00

[Privately confidential]



Due Diligence

Toolkit: <https://github.com/markoer73/M-A>



“Capture” of Security Controls

- » 13 Domains to verify
 - 1. Digital Identities
 - 2. Admin Accounts
 - 3. Endpoints/Client Systems
 - 4. Servers
 - 5. Networks
 - 6. Hosting
 - 7. Email
 - 8. Data Recovery
 - 9. Boundary Defenses
 - 10. Assets Inventory
 - 11. Operational Security
 - 12. Physical Security
 - 13. Wireless Networks



Example of Policy Requirement

Domain	Verification	How-to	Objectives	Minimum Acceptable Level
Digital Identities	<p>Verify status of identities in main identity store (use of unique IDs, generic accounts, password policy, Groups' usage, GPOs, Federations, etc.). Verify if anything is outside of the main identity store (e.g. VPN accounts, Cloud accounts, supplier accounts, etc.).</p>	<ul style="list-style-type: none"> Interview with IT admins from Target. Snapshot of information from AD/LDAP. Interview with business units which manage other tools (Cloud etc.), to understand how this is managed 	<ul style="list-style-type: none"> Ensure appropriate controls are in place to protect Target environment and data Get an idea of the complexity of the DI structure of the Target. Understand usage of Cloud applications and identities. Understand how restriction of access to information happens in Target. 	<ul style="list-style-type: none"> There is a Directory Service Unique IDs are used Permissions are assigned via Groups in the Directory Service Service and Cloud accounts are gathered, minimized, and under control Sensitive files are shared in a secure way
Admin Accounts	<p>Verify status of admin account management in main identity store, if managed there.</p> <p>Verify if anything is outside of the main identity store (e.g. VPN accounts, Cloud accounts, supplier accounts, etc.)</p>	<ul style="list-style-type: none"> Interview with IT admins from Target. Snapshot of information from AD/LDAP and other tools. 	<ul style="list-style-type: none"> Ensure admin account controls are defined, implemented and reviewed to protect systems and data Understand how IT administrative actions are performed, what the procedures and practices are, and who has the ownership and responsibility. 	<ul style="list-style-type: none"> Admin accounts are managed under a Directory Service Admin accounts are unique for each admin Central ownership of who gets appropriate rights Process for removing rights as appropriate



Example of Interview Questions

Domain	Minimum Acceptable Level	Key Topics for Discussion
Digital Identities	<ul style="list-style-type: none">• Directory Services of any kind are used• Unique IDs are used• Permissions are assigned via Groups in the Directory Service• There is an adequate password policy in place• Service and Cloud accounts are gathered, minimized, and under control• Sensitive files are shared in a secure way	<ul style="list-style-type: none">• How many people are present in the company? Get overview of employees' org chart/roles, and how many people are in IT and Security.• How old is the company? Get brief history, acquisitions, etc.• Which DS is used? (AD, which version?)• Get overview of Groups, GPOs, shared accounts, shared mailboxes, federated services, password policy (for AD, request screenshots).• Is every system and device connected to DS and follow password policy, or there are systems which have their own passwords (e.g. Wi-Fi, network devices, etc.)?• What is the process by which Group ownership, permissions and accesses to systems and applications are granted?• Get overview of Cloud services used and how accounts are managed, if SSO is used and how, especially concerning files and documents sharing with third parties.• Is Cloud Sharing such as Box, Dropbox etc. being used?
Admin Accounts	<ul style="list-style-type: none">• Admin accounts are managed under a Directory Service• Admin accounts are unique for each admin• Central ownership of who gets appropriate rights• Process for removing rights as appropriate	<ul style="list-style-type: none">• Get overview of how administration is performed, if AD Groups and GPOs are used, if shared accounts and/or shared mailboxes are used for admin accounts• Understand how permissions are granted and removed from users as their work and function changes in the company



1. Control Required Practice Validation

Company: [REDACTED] Area: General IT Controls [REDACTED] Reference No.: [REDACTED]

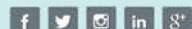
Assigned To:	Marco Ermini	Targeted Completion Date:	[REDACTED]
Phone:	[REDACTED]	Closed Date:	[REDACTED]
Date of Validation:	[REDACTED]		
Validation Completed By:	[REDACTED]		
Period Tested	From:	To:	[REDACTED]
Reviewed By:	[REDACTED]	Date:	[REDACTED]

2. Summary of the Outcomes

Description	Overall Status
In March 2016 we have tested the target for acquisition in project [REDACTED] in order to perform M&A due diligence activities. The results are the followings:	Green
Security Impact:	
<ul style="list-style-type: none">• High security Impact – to be addressed with more urgency:<ul style="list-style-type: none">◦ Endpoint/Client Systems, Operational Security• Medium security impact – to be addressed with normal priority:<ul style="list-style-type: none">◦ Data Recovery functions, Remote Terminal Services access, Servers Environment, Networks, Email• Low security impact – to be addressed with lower priority:<ul style="list-style-type: none">◦ Digital Identities, Administrative Accounts, Hosting, Inventory, Wireless, Boundary defenses	Green
Processes Impact:	
<ul style="list-style-type: none">• Medium impact on processes:<ul style="list-style-type: none">◦ Hosting, Inventory, Wireless, Procurement process for equipment, Servers Environment, Networks, Email, Boundary defenses, Operational Security• Low impact on processes:<ul style="list-style-type: none">◦ Digital Identities, Administrative Accounts, Data Recovery functions	Green
Cost Impact:	
<ul style="list-style-type: none">• May not incur an additional costs:<ul style="list-style-type: none">◦ Digital Identities, Administrative Accounts, Hosting, Inventory, Wireless, Servers Environment, Email, Physical Security• May incur in additional costs:<ul style="list-style-type: none">◦ additional storage for backup, dedicated network connectivity towards [REDACTED] wireless equipment (not urgent), possible replacement/reimage of all client system, network equipment and firewalls aligned to current standards, additional feeds into the SIEM and external MSSP	Green

Risk Assessment

- » Management Summary with a clear status
- » Clearly indicate the area that will need additional attention
- » Especially indicate where the additional costs will incur (e.g. new wireless equipment, re-imaging of the endpoints, reimplementation of firewall, etc.)



4. Controls which will require more adjustments (insufficient)

7. Endpoint/Client Systems

- Endpoints require being standardised to [REDACTED] ones.
- Endpoints will require disk level encryption.
- Endpoints will require antimalware protection to be elevated to [REDACTED] standards.
- Remote access via Terminal Services need to receive a security assessment, can be potentially insecure.

Evaluation:

- Security Impact: high.
- Process impact: medium.
- Cost impact: the cost of client replacement, processes alignment including procurement, and field service will have a cost impact.

8. Servers Environment

- Servers will need to be aligned with [REDACTED] standards in terms of patch distribution (SCCM) and receive periodic and urgent security patches when available.
- Servers will require antimalware protection to be elevated to [REDACTED] standards.

Evaluation:

- Security Impact: medium.
- Process impact: medium.
- Cost impact: it may not incur an additional cost, and actually concur into a consolidation.

9. Networks

- Linux Firewall and SOHO equipment such as FritzBox will need to be upgraded to [REDACTED] standard.
- Should be evaluated whether the DMZ is still required once joining [REDACTED] or should it be moved to [REDACTED]

Evaluation:

- Security Impact: medium.
- Process impact: medium.
- Cost impact: the cost of new network equipment must be budgeted, as well as connectors to [REDACTED] and other required licenses.

Impact Assessment

» Indicate the kind of impact:

- Security
- Processes
- Costs

» Indicate expected remediation, aligned with IT

» If not possible to estimate costs immediately, indicate how they should be calculated (e.g. need to provision new firewall cluster)



Summarize Findings aligned with IT – in one Slide



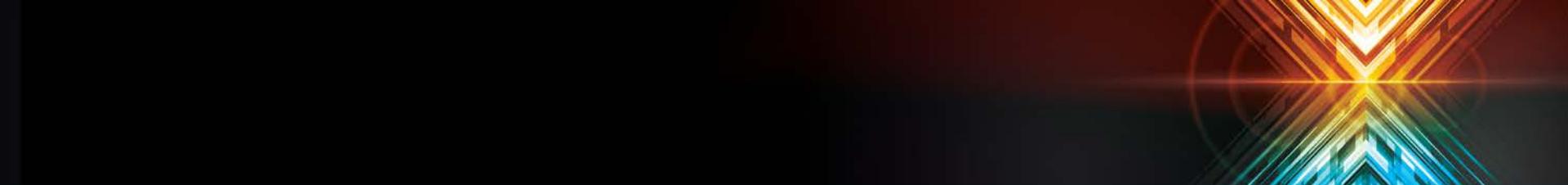
Due Diligence / Integration – IT

- No significant IT issues to acquisition or challenges to integration found
 - Microsoft server software license transfer not completed yet
 - Maintenance contracts expired for major infrastructure components
- Desktop Environment
 - Small (24) workforce with company owned laptops/desktops (3 yrs average) and mobile devices; Remote desktop access for most users; Office 2013
- Server / Infrastructure Environment
 - Minimal on premise computer systems (small data room / 2 racks)
 - Microsoft Small Business 2008 Premium (Exchange, AD, DNS, etc.)
 - Most equipment EOL (4+ years)
 - 10x virtual servers on local hardware
- Production Systems
 - ERP: Microsoft Dynamics C5 – on premise
 - CRM: Microsoft Dynamics CRM – hosted at [REDACTED] DataCenter
 - Old CRM: Superoffice - to be retired in 12/2015
 - Webshop: www.[REDACTED].dk hosted at [REDACTED]

Costs aligned with IT for integration

Item	FY2016	
	Capital	recurring/monthly
Day one need		
Vodafone MPLS Line (10Mbit)	2.000,00 €	1.500,00 €
Firewall (Palo Alto)	12.000,00 €	100,00 €
Cisco Core Switch	20.000,00 €	100,00 €
Cisco Bridging Router	2.000,00 €	
Cisco Wireless Controller	2.500,00 €	
Cisco Access Point (3x)	1.500,00 €	
Consulting (ext. Resources)	5.000,00 €	
	45.000,00 €	1.700,00 €
FY2017		
Item	Capital	recurring/monthly
10x Notebook EOL Replacement	11.000,00 €	
Option 1: Build up Infrastructure on premise		
SCCM Server (Distribution Point)	4.000,00 €	50,00 €
2x physical servers (VMWare)	10.000,00 €	100,00 €
Storage (VNX)	30.000,00 €	250,00 €
Backup Data Domain		500,00 €
	44.000,00 €	900,00 €
Option 2: Move applications into a Managed Data Center		
5x hosted virtual servers		3.000,00 €
Storage for hosted applications		1.000,00 €
	0,00 €	4.000,00 €





Connect

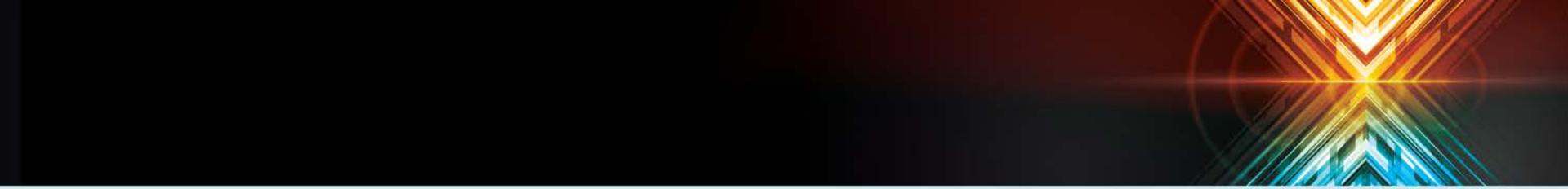
CSX™ 2017
EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT



Starting to work in Clear Sight

- » The news is out
- » Information Completeness is paramount
- » An Integration Plan is proposed
 - Technical Integration
 - Networks, PCs, applications, data centers, hosting...
 - Business Processes and Systems
 - Timing
- » The Integration Plan must also negotiate from an “as-is” to a “to-be” state for the Target





Combine



Target Characteristics	Security Guidelines	SLAs
<ul style="list-style-type: none"> ► Little to no geographical diversity ► No separate legal entities ► No/limited need to keep the same facilities ► No/limited to keep the existing technologies ► Purchased for limited product portfolio, technology, talent, or local presence 	<ul style="list-style-type: none"> ► Baseline security controls ► Target is fully absorbed into IT infrastructure ► All IT labor is absorbed into IT global business units 	<ul style="list-style-type: none"> ► Security controls established or confirmed in less than 100 days
<ul style="list-style-type: none"> ► Similar to previous kind, but Target has certain identifiable complexities that require specific sensitivity during integration ► Fewer than 500 employees ► Needs to be stand-alone for a certain period of time ► During stand-alone time, Target maintains defined non-compliances ► Supports its own IT infrastructure during the stand-alone phase <p>MEDIUM</p>	<ul style="list-style-type: none"> ► Integration of Target may be full, hybrid, or standalone ► All IT labor is absorbed into IT global business units 	<ul style="list-style-type: none"> ► Operation integration of some IT infrastructure may take +180 days ► Processes may take 3 to 9 months
<p>LARGE</p> <ul style="list-style-type: none"> ► More than 500 employees ► Relatively large operations ► Significant multinational presence and subsidiaries ► Target contains certain identifiable complexities that require specific sensitivity during integration 	<ul style="list-style-type: none"> ► Integration of Target may be full, hybrid, or standalone ► IT labor can stay funded by Target company 	<ul style="list-style-type: none"> ► Operation integration of some IT infrastructure may take +180 days ► Customized integration plan ► IT Support is shared ► Processes take more than 12 months



Combining the two companies

- » Resources, staffing, processes, and systems are combined
- » Business processes are as much as possible leveled
- » IT tools are unified
- » ***Active Directory merging strategy is key!***
- » The Target company has comparable / same security
- » Exceptions are documented and signed off by leadership (executives, CISO)
- » Agreed-upon designs are implemented
- » Operations — including InfoSec — are turned to standard support
- » Weekly or recurring meetings can be setup to assess progresses



Planning the Active Directory Integration

- » Training for the technicians performing the migration
- » Scheduled outages
- » Companies' cultural differences such as who's allowed access to AD and Exchange, or how file system security is set
- » Network differences between the two sites
- » Network, AD, or Exchange anomalies
- » Customer and employee communication



Pain Points in Active Directory Integration

- » Deciding the strategy
 - Integrate the Target into the Acquiring
 - Build a new, combined AD
 - Migrate legacy objects into a new AD
- » ***One Company, One Email!***
 - Free/Busy Information
 - Exchange/Lync/Office/AD versions
 - Office 365?
- » External Federations/Partners/ADFS?
- » DNS configuration/forwarding
- » SID history/filtering
- » Evaluate purchase of a dedicated AD migration/upgrade tool





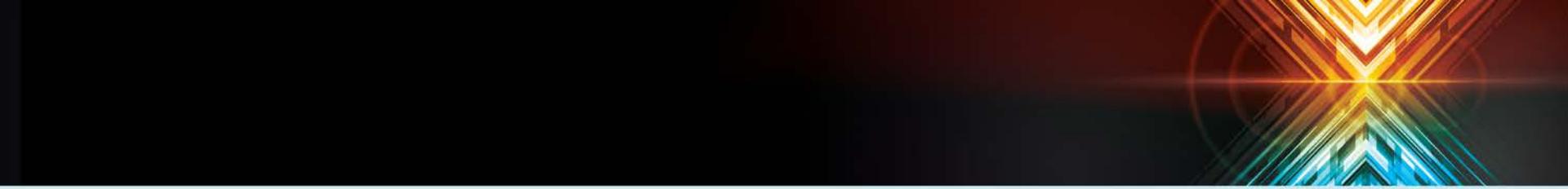
Adjusting Policies



Merging Policies

- » Safeguards against disgruntled employees
- » New employee contracts
 - Are existing Policies still relevant?
 - Are we “dumbing down” their security?
- » Existing employee contracts
 - Do they protect you?
 - Do they meet new relationship?
- » Identify key policies — yours vs theirs
 - Work with Legal Departments





Merging InfoSec



The New Security Department

- » Cost/Budgeting
 - Pre-merger: OpEx
 - Merger: CapEx, Processes
 - Post-merger: Optimization
- » Communications



What if I am on the weak side?

1. Identify specific strengths that can be useful in the merging
 - Experience from security incidents
 - Technological implementations
 - Local knowledge and compliance
2. Be prepared to learn
 - What is the current Cyber Security philosophy?
 - Who is taking security-related decisions?
3. Don't rush your career decisions
 - Can bring new opportunities
 - Meet the new management





Leveraging the Cloud



Cloud Email

The screenshot shows a web browser window titled "Inbound Routes" with the URL <https://clients.com/Configuration>Email-Security/SelfServe/Se...>. The top navigation bar includes links for Dashboard, Users and Groups, Services, Reports, Tools, Support, and a "What's New" button. The main content area displays the "Inbound Routes" page. A yellow banner at the top says "Introducing Symantec Advanced Threat Protection: Email". Below it, a message states: "The IP address of each server that receives email from external sources must be registered. Default routes are associated with all of your registered domains. You can also define custom routes for specific domains." A status message indicates "At least one inbound route is registered". The "Registered Default Inbound Routes" section lists four entries:

Priority	IP Address	Date Registered	Delete Route	Technical Check	Change Priority	Can Promote to Primary
1	mx[REDACTED].de	14 Feb 2005		Check		No
2	mx[REDACTED].com	14 Feb 2005	Delete	Check	▲ ▼	No
3	inbound-mx[REDACTED].com	19 Jul 2012	Delete	Check	▲ ▼	No
4	mx[REDACTED].com.au	14 Feb 2005	Delete	Check	▲ ▼	No

Buttons at the bottom include "Check New", "Add and Check New", and "Domain List". A note below the table states: "The following domains are registered with the following routes."



**CSX™ 2017
EUROPE**
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

SaaS WAF/

Hello, marco.ermi@ | logout

Sites | Account | DNS Zones | Support | Documentation

My Sites: 7-Day Statistics

Website	Traffic Human Visits Bot Visits	Threats	Bandwidth Cached Total	Status	
[REDACTED]	127.85	Bad Bots: 1	134.7MB	Enabled	STATS >
	7,366 30,617	Bad Bots: 1844 Illegal Resource Access: 2	13.5GB 15.1GB	Enabled	STATS >
	265.188	IncapRules: 150	2.6MB 574MB	Enabled	STATS >
	3.2	-	24.1KB	Enabled	STATS >
	5	-	111.3KB	Enabled	STATS >
	5,564 8,979	Bad Bots: 2902 Illegal Resource Access: 1	10.9GB	Enabled	STATS >
	11,400 8,933	Bad Bots: 682 Illegal Resource Access: 10 SQL Injection: 1	13.5GB	Enabled	STATS >



CSX™ 2017
EUROPE

CYBERSECURITY NEXUS

AN ISACA CYBER EVENT

Moving to a Cloud-Based ERP or Email Solution

- » Traditional M&A dogma is “transition, then transform”
- » Companies however are leveraging migration to key technologies to the Cloud during the M&A process as an enabler
- » Can simultaneously replace aging, capital-intensive technology with a subscription-based operating model
- » Ideal also for divestitures
- » Boarding is considerably faster and cheaper than traditional on premise solutions (Accenture estimates 30% for both)
- » Ultimate flexibility during a post-deal transition



Cloud WA

Hello, marco.ermini@... [logout](#)

Sites | Account | DNS Zones | Support | Documentation

e.g. www.example.c [Dashboard](#) [Events](#) [Settings](#)

Site settings

[Save](#)

SSL Support

Certificate Type	Incapsula generated certificate i	Custom certificate i
Certificate Status	Not active	Active
Actions	configure details remove	

Strict-Transport-Security (HSTS) [i](#)

Enable Max-age [i](#)
 Include Sub-Domains [i](#)
 Pre-load [i](#)

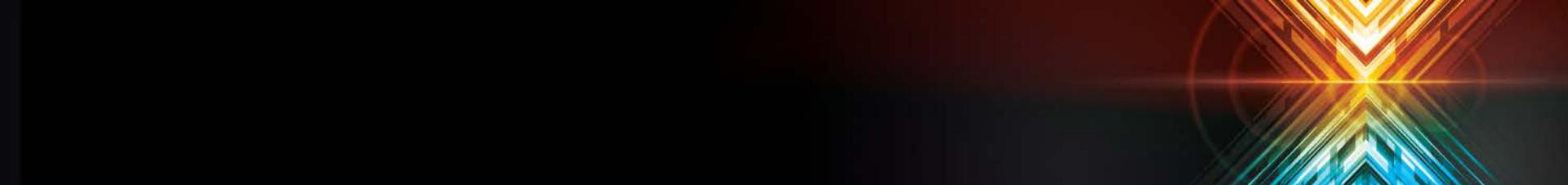
HTTP/2 [i](#)

Enable HTTP/2 [i](#)

Redirection

Redirect <http://> [to https://](#) [i](#)

Origin Servers [General](#) [Monitoring](#) [IncapRules](#) [Login Protect](#)

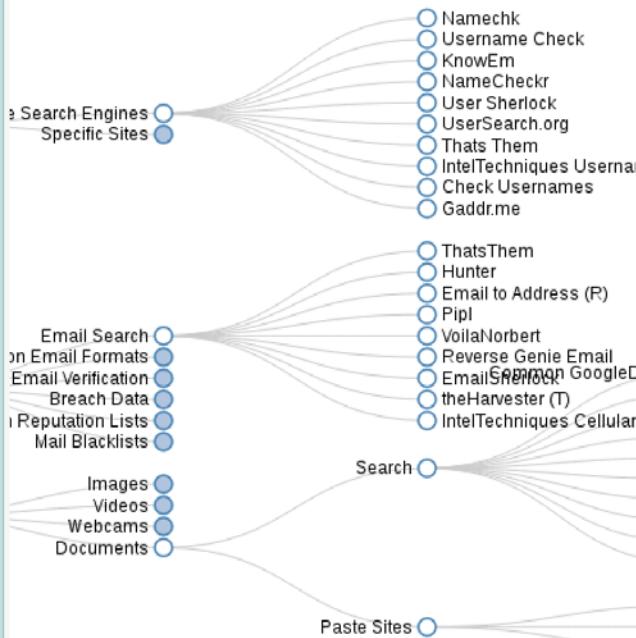


Open Source information gathering

Backup Slides



OSINT Framework



Open Source Intelligence

- » Collection of free tools and source of information
- » They divide into
 - Tools which can run locally
 - Search Engine “dorking” (e.g. Google hacking)
 - Semi-closed sources
 - Exploitation of sites which have originally other purposes (e.g. social networks, dating sites...)

METASPLOIT recon-ng

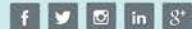
```
[2] Exploitation modules
[recon-ng][default] > show modules

Discovery
-----
discovery/exploitable/http/dnn_fcklinkgallery
discovery/exploitable/http/generic_restaurantmenu
discovery/exploitable/http/webwiz_rte
discovery/info_disclosure/dns/cache_snoop
discovery/info_disclosure/http/backup_finder
discovery/info_disclosure/http/google_ids
discovery/info_disclosure/http/interesting_files

Exploitation
-----
exploitation/injection/command_injector
exploitation/injection/xpath_bruter

Recon
-----
recon/contacts/enum/http/api/haveibeenpwned
recon/contacts/enum/http/api/rapportive
recon/contacts/enum/http/web/dev_diver
recon/contacts/enum/http/web/namechk
recon/contacts/enum/http/web/pwnedlist
recon/contacts/enum/http/web/should_change_password
recon/contacts/gather/http/api/jigsaw/point_usage
recon/contacts/gather/http/api/jigsaw/purchase_contact
recon/contacts/gather/http/api/jigsaw/search_contacts
recon/contacts/gather/http/api/linkedin_auth
recon/contacts/gather/http/api/twitter
recon/contacts/gather/http/api/whois_pocs
recon/contacts/gather/http/web/jigsaw
recon/contacts/gather/http/web/pgp_search
recon/contacts/support/add_contact
recon/contacts/support/mangle
recon/creds/enum/http/api/leakdb
recon/creds/enum/http/api/noisette
```

AN ISACA CYBER EVENT



FOCA Search

Whitehouse.gov - FOCA Free 3.2

Project Tools Options TaskList About Donate

Whitehouse.gov Network Clients (0) Servers (3) Domains whitehouse.gov Related Domains akamatechnologies.com apple.com Roles Vulnerabilities Metadata Documents (0/1097) Metadata Summary

Clean your OpenOffice documents with OOMetaExtractor

Search engines: Google, Bing, Exalead

Extensions: doc, xls, ppt, docx, xlsx, sxi, pps, ppbx, sxiw, odt

Custom search

ID	Type	URL	Download	Download Date	Size	Analyzed	N
1029	pdf	http://www.whitehouse.gov/sites/default/files/uploads...	X	-	-	X	-
1030	pdf	http://www.whitehouse.gov/sites/default/files/omb/as...	X	-	-	X	-
1031	pdf	http://www.whitehouse.gov/sites/default/files/omb/as...	X	-	-	X	-
1032	pdf	http://www.whitehouse.gov/sites/default/files/omb/as...	X	-	-	X	-
1033	pdf	http://www.whitehouse.gov/sites/default/files/micros...	X	-	-	X	-
1034	pdf	http://www.whitehouse.gov/sites/default/files/omb/as...	X	-	-	X	-
1035	pdf	http://www.whitehouse.gov/sites/default/files/omb/as...	X	-	-	X	-
1036	pdf	http://www.whitehouse.gov/sites/default/files/micros...	X	-	-	X	-
1037	pdf	http://www.whitehouse.gov/sites/default/files/omb/as...	X	-	-	X	-
1038	pdf	http://www.whitehouse.gov/sites/default/files/docs/d...	X	-	-	X	-
1039	pdf	http://www.whitehouse.gov/sites/default/files/omb/as...	X	-	-	X	-
1040	pdf	http://www.whitehouse.gov/sites/default/files/omb/as...	X	-	-	X	-

Time Source Severity Message

3:39:42 Fuzzer medium File found on http://m.whitehouse.gov:80/robots.txt: http://m.whitehouse.gov/?q=logout/

3:39:42 Fuzzer medium File found on http://m.whitehouse.gov:80/robots.txt: http://m.whitehouse.gov/?q=node/add/

3:39:42 Fuzzer medium File found on http://m.whitehouse.gov:80/robots.txt: http://m.whitehouse.gov/?q=search/

3:39:42 Fuzzer medium File found on http://m.whitehouse.gov:80/robots.txt: http://m.whitehouse.gov/?q=user/password/

3:39:42 Fuzzer medium File found on http://m.whitehouse.gov:80/robots.txt: http://m.whitehouse.gov/?q=user/register/

3:39:42 Fuzzer medium File found on http://m.whitehouse.gov:80/robots.txt: http://m.whitehouse.gov/?q=user/login/

Conf Deactivate AutoScroll Clear Save log to File

Search done

Job Posting's Harvesting

The screenshot shows a LinkedIn job posting for a Network Administrator. The job description lists responsibilities such as performing software updates, working on projects, developing documentation, and looking proactively for improvements. It also specifies requirements like a university degree, several years of network administration experience, and a good understanding of various protocols and technologies. The posting is categorized as full-time and in the Information Technology function. A large portion of the job requirements section is highlighted with red boxes, specifically mentioning Cisco products (Nexus family, ASA, Catalyst switches), BIG-IP F5, Next-Generation Firewalls (Checkpoint, Juniper, Palo Alto), and Linux operating systems.

Network Administrator (m/f)

Sicuro | https://www.linkedin.com/jobs/view/ [REDACTED]

Search

Home My Network Jobs Messaging Notifications Me

Requests, network configurations, troubleshooting, etc.

- Perform software updates/upgrades on the network devices
- Work on projects and assignments from a supervisor
- Develop new and maintain the existing documentation (diagrams, job-aids, procedure, etc.)
- Look proactively for network improvements

Employment Type
Full-time

Job Functions
Information Technology

Your profile

- University degree or equivalent experience
- Several years of network administration or implementation experience
- Very good understanding of TCP/IP model
- Very good understanding of general protocols and technologies: VLANs, L2 protocols (CDP, UDLD, etc.), trunking, etherchannels, vPC, 802.1D STP and flavors, FHRPs, WLAN, IP Addressing & subnetting, DHCP, OSPF, BGP, Static routing, IPSec VPN, ACL, NAT, SSL, DNS, IPv6, L7 Load balancing
- Experience in configuring, managing and troubleshooting Cisco network products such as [REDACTED] Nexus family, ASA, Catalyst switches
- Experience in configuring, managing and troubleshooting [REDACTED] BIG-IP F5 (1 M, GTM)
- Experience in configuring, managing and troubleshooting Next-Generation Firewalls (Checkpoint, Juniper, Palo Alto is a plus)
- Basic experience of using Linux operating systems and virtualization basics
- ITIL aware
- Good interpersonal and communication skills
- Ability to work independently with minor guidance as well as Team player
- Excellent command of English, German is highly appreciated

Job Posting's Harvesting

Marco (Gmail)

Jobs für Palo Alto in München, x

Sicuro https://www.glassdoor.de/Job/münchen-palo-alto-jobs-SRCH_IL... ☆

Jobs bei Palo Alto in München, Bayern 16 Jobs

Filter Suchradius X

(Senior-) IT-Consultant (m/w) Arbeitsort: München
GmbH - München Schnellbewerbung vor 1 Tagen
3,0 ★

Systemadministrator Netzwerk (m/w) München vor 5 Tagen
3,4 ★

Solution Expert for Internet of Things (IoT) Co-Innovation within the München vor 26 Tagen
4,4 ★

System Engineer IT Security (m/w) im Raum Augsburg Garching b.München vor 10 Tagen
3,4 ★

Netzwerkadministrator mit Schwerpunkt Security m/w München Schnellbewerbung

Auf Unternehmensseite bewerben Speichern

Dein Profil:

- Du bringst neben deiner Begeisterung für Technik ein erfolgreich abgeschlossenes Informatikstudium oder eine vergleichbare Ausbildung mit.
- Du hast eine offene Einstellung zu den Kernwerten der AG.
- Du hast Erfahrungen mit größeren Netzwerken.
- Du verfügst über gute Kenntnisse in der Cisco Welt (FEX / Fabric Path / VPC / VDC / OSPF), Cisco ASA Firewall (VPN), Cisco ASR 1K/9K Router (BGP internet peering), Cisco Catalyst Switches.
- Wünschenswert sind Kenntnisse in Palo Alto firewall, Checkpoint firewall, Juniper/Pulse Secure VPN gateway, F5 Loadbalancer, DELL/Force10 Switches & Bladecenter Switches.
- Du zeigst Bereitschaft, Dich mit anderen Themen wie Storage, Backup, VM auseinanderzusetzen.
- Du verfügst über erste Kenntnisse in agilen Arbeitsmethoden.
- Vorteilhaft ist das Umgang mit Tools wie JIRA und Confluence.
- Deutsch und Englisch fließend in Wort und Schrift.

Unser Angebot:

CYBERSECURITY NEXUS EUROPE
AN ISACA CYBER EVENT

Job Interviews' Harvesting

Sicuro <https://www.glassdoor.de/Vorstellungsgespräch/>

Übersicht 3,8 Tsd Bewertungen 3,1 Tsd Jobs 9,5 Tsd Gehälter 1,1 Tsd Vorstellungsgespräche 1,1 Tsd Zusatzleistungen Mehr Beobachtet +

Kein Angebot Negative Erfahrung Durchschnittl. Gespräch

Bewerbung

Ich habe mich über einen Personalvermittler beworben. Vorstellungsgespräch absolviert im April 2017 bei [REDACTED] VA (Vereinigte Staaten von Amerika).

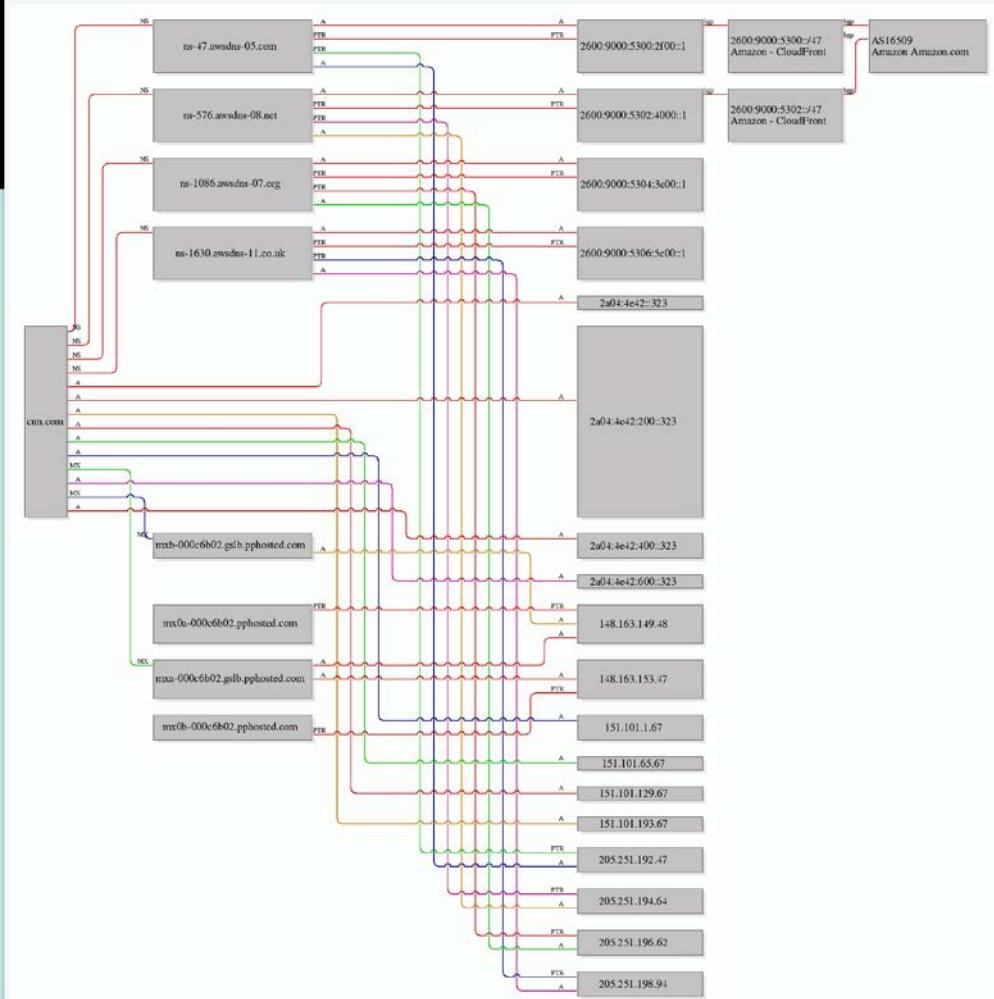
Vorstellungsgespräch

I was contacted by [REDACTED]. They had found my resume online. I was told the company was looking for several [REDACTED] Dynamics CRM developers as soon as possible. The job description matched my skill set very closely. I was told someone will contact me to setup an interview within couple of days. I received an email a few days later with instructions to dial in to conduct an interview without coordinating with me prior to the interview time. I received a phone call in the morning of my interview by another recruiter. When I told her that nobody had coordinated with me and I would not be available for the interview, she apologized and setup the interview for another day. I had 45 minutes talk with 3 people over the phone. One interviewer was a lady who said she was not technical but also said that it seemed like I had not done a lot of technical work on my last job because of my title at my last job (CRM Administrator). I told her that my title did not represent my work. The company that I was working for was a small company and the title was misleading and as a matter of fact I had done technical work for them. The other 2 interviewers sounded young but they said they were Architects. I had a hard time understanding them over the phone too. The questions

The screenshot shows a web browser window with the URL <https://www.robtex.com/dns-lookup/cnn.com>. The page title is "cnn.com". A navigation bar at the top includes links for "Robtex", "DNS", "com", and "cnn". Below the title, there is a search bar containing "cnn.com" and a row of buttons: "Search" (highlighted in green), "Summary", "Whois" (highlighted in green), "Blacklists", "Forward", "Reverse", "Similar", "Scorecard", "Shared", "Graph", "Route", and "AS". A tip message states: "⚠️ TIP: To find whois-info and blacklists for cnn.com, click on the corresponding green buttons above. If you are missing anything else from the old interface, it is located [HERE](#) for a while longer." The main content area is titled "Records" and displays a table with the following data:

TYPE	HOSTNAME	IP	PTR	GEO-NETWORK
		2a04:4e42::323	-	2a04:4e42::/36 AS54113 Fastly Fastly, Inc.
				2a04:4e42::/36 AS54113 AN ISACA CYBER EVENT

At the bottom right, there are social media sharing icons for Facebook, Twitter, LinkedIn, and Google+.



Harvesting of Corporate Emails

```
e Edit View Search Terminal Help  
@kali2:~# theharvester -d com -b all -h  
Shared  
*****  
theHarvester Ver. 2.7  
coded by Christian Martorella  
edge-Security Research  
martorella@edge-security.com  
*****  
  
L harvest..  
Searching in Google..  
Searching 0 results...  
p Suite  
Searching 100 results...  
Searching in PGP Key server..  
Searching in Bing..  
Searching 50 results...  
Searching 100 results...  
Searching in Exalead..  
Searching 50 results...  
Searching 100 results...  
Searching 150 results...  
  
SSP.txt  
Emails found:  
-----  
ssehaar@[REDACTED].com  
e.Macdonald@[REDACTED].com  
rnwalds@[REDACTED].com  
Comas@[REDACTED].com  
dwng@[REDACTED].com  
dersong@[REDACTED].com  
tson@[REDACTED].com  
denouri@[REDACTED].com  
cey@[REDACTED].com  
uiry@[REDACTED].com  
pcenter@[REDACTED].com  
o@[REDACTED].com  
ntaniello@[REDACTED].com
```

Gathering of domain names

```
root@kali2: ~
File Edit View Search Terminal Help
root@kali2:~# dnsmap [REDACTED].com
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for [REDACTED].com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

connect.[REDACTED].com
IP address #1: [REDACTED].212.211

go.[REDACTED].com
IP address #1: [REDACTED].213.48

helpdesk.[REDACTED].com
IP address #1: [REDACTED].72.99

portal.[REDACTED].com
IPv6 address #1: [REDACTED]::5ef5:6c55

portal.[REDACTED].com
IP address #1: [REDACTED].108.85

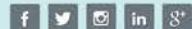
www.[REDACTED].com
IP address #1: [REDACTED].185.240

[+] 6 (sub)domains and 6 IP address(es) found
[+] completion time: 607 second(s)
root@kali2:~#
```

Gathering of domain names

```
root@kali2: ~
File Edit View Search Terminal Help
root@kali2:~# dnsrecon -d .com
[*] Performing General Enumeration of Domain: .com
[-] DNSSEC is not configured for .com
[*] SOA com 35.18
[*] NS com 125.130
[-] Recursion enabled on NS Server com 125.130
[*] NS com 193.104
[-] Recursion enabled on NS Server com 193.104
[*] NS com 178.25
[-] Recursion enabled on NS Server com 178.25
[*] NS com 34.55
[-] Recursion enabled on NS Server com 34.55
[*] NS com 20.104
[-] Recursion enabled on NS Server com 20.104
[*] NS com 192.24
[-] Recursion enabled on NS Server com 192.24
[*] MX mail.protection.outlook.com 180.74
[*] MX mail.protection.outlook.com 180.106
[*] A 45.79.185.240
[*] TXT v=spf1 ip4:255.114 ip4:194.4 ip4:246.30 ip4:171.34 ip4:74.204.0/22 ip4:168.0/23 include: com include:spf.protection.outlook.com include: com
m -all
[*] Enumerating SRV Records
[*] SRV _sip._tls. com sipdir.online.lync.com 52.112.192.139 443 1
[*] SRV _sip._tls. com sipdir.online.lync.com 2603:1027:0:4::b 443 1
[*] SRV _sip._tls. com sipdir.online.lync.com 2603:1027:0:8::b 443 1
[*] SRV _sip._tls. com sipdir.online.lync.com 2603:1027:0:3::b 443 1
[*] SRV _sip._tls. com sipdir.online.lync.com 2603:1027::b 443 1
[*] SRV _sip._tls. com sipdir.online.lync.com 2603:1027:0:7::b 443 1
[*] SRV _sip._tls. com sipdir.online.lync.com 2603:1027:0:6::b 443 1
[*] SRV _sip._tls. com sipdir.online.lync.com 2603:1027:0:1::b 443 1
[*] SRV _sip._tls. com sipdir.online.lync.com 2603:1027:0:9::b 443 1
[*] SRV _sipfederationtls._tcp. com sipfed.online.lync.com 52.112.192.139 5061 1
[*] SRV _sipfederationtls._tcp. com sipfed.online.lync.com 2603:1027::b 5061 1
[*] SRV _sipfederationtls._tcp. com sipfed.online.lync.com 2603:1027:0:9::b 5061 1
[*] SRV _sipfederationtls._tcp. com sipfed.online.lync.com 2603:1027:0:1::b 5061 1
[*] SRV _sipfederationtls._tcp. com sipfed.online.lync.com 2603:1027:0:4::b 5061 1
[*] SRV _sipfederationtls._tcp. com sipfed.online.lync.com 2603:1027:0:8::b 5061 1
[*] SRV _sipfederationtls._tcp. com sipfed.online.lync.com 2603:1027:0:6::b 5061 1
[*] SRV _sipfederationtls._tcp. com sipfed.online.lync.com 2603:1027:0:7::b 5061 1
[*] SRV _sipfederationtls._tcp. com sipfed.online.lync.com 2603:1027:0:3::b 5061 1
[*] 18 Records Found
root@kali2:~#
```

AN ISACA CYBER EVENT



Old (and new) fashion scanning

```
root@kali2: ~
File Edit View Search Terminal Help
root@kali2:~# nmap 246.204
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-04 10:26 CEST
Nmap scan report for 246.204
Host is up (0.20s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    filtered ssh
554/tcp   open  rtsp
7070/tcp  open  realserver
Nmap done: 1 IP address (1 host up) scanned in 27.33 seconds
root@kali2:~#
root@kali2:~# zmap 246.204 -p 123
Apr 04 10:30:04.616 [WARN] blacklist: ZMap is currently using the default blacklist located at /etc/zmap/blacklist.conf. By default, this blacklist excludes locally scoped networks (e.g. 10.0.0.0/8, 127.0.0.1/8, and 192.168.0.0/16). If you are trying to scan local networks, you can change the default blacklist by editing the default ZMap configuration at /etc/zmap/zmap.conf.
Apr 04 10:30:04.621 [WARN] zmap: too few targets relative to senders, dropping to one sender
Apr 04 10:30:04.795 [INFO] zmap: output module: csv
Apr 04 10:30:04.796 [INFO] csv: no output file selected, will use stdout
0:00 0%; send: 0 0 p/s (0 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:01 13%; send: 1 done (29 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:02 25%; send: 1 done (29 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:03 38%; send: 1 done (29 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:04 50%; send: 1 done (29 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:05 63% (3s left); send: 1 done (29 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:06 75% (2s left); send: 1 done (29 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:07 88% (1s left); send: 1 done (29 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
0:08 100% (0s left); send: 1 done (29 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
Apr 04 10:30:13.870 [INFO] zmap: completed
root@kali2:~#
```



Maltego

Start a Machine X

STEPS

1. Choose machine
2. **Specify target**

SPECIFY TARGET: Please provide parameters for the machine to target.

The Company Stalker machine requires the following inputs:

Domain Name

[Back](#) [Next >](#) **Finish** [Cancel](#)

Maltego

Start a Machine X

CHOOSE MACHINE: Please select the machine to run from the list below.



Prunes enrichment transform to allow for only displaying Tags

Company Stalker [Domain]
This machine will try to get all email addresses at a domain th...

Domain Analysis [Domain]
Pulls all relevant information from PassiveTotal About a given ...

Domain Explorer [Domain]
Pulls all relevant information from PassiveTotal about a given ...

Domain Hunter [Domain]

Show on startup

Show on empty graph click

< Back Next > Finish Cancel

Maltego

Start a Machine X

CHOOSE MACHINE: Please select the machine to run from the list below.



STEPS

- 1. Choose machine**
- 2. Specify target**

This performs a level 1 (fast, basic) footprint of a domain.

Footprint L2 [Domain]
This performs a level 2 (mild) footprint of a domain.

Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It take...

Footprint XXL [Domain]
This machine is built to work on really large targets that's hosti...

Show on startup

Show on empty graph click

< Back **Next >** **Finish** **Cancel**

Maltego Kali Linux Edition 4.0.11

Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows

Entity Palette <> X

Devices

- Device A device such as a phone

Infrastructure

- AS An internet Autonomous System
- Banner Banner
- DNS Name Domain Name System
- Domain An internet domain

Run View <> X

Entity Selection

- Select All
- Select None
- Invert Selection

Number of Results 12 50 255 10k

Quick Find Find in Files

Machines

Collaboration

Import | Export

Windows

Select by Type

Select Children

Add Parents

Add Neighbors

Add Children

Add Path

Select Neighbors

Select Similar Siblings

Select Parents

Select Bookmarked

Reverse Links

Entity Selection

Layout

Home New Graph (5) X

100%

Select netblock

Choose the netblocks belonging to your target - we'll run reverse DNS on the selected ones.

Netblocks

	Type	In
1	Netblock	6
1	Netblock	6
1	Netblock	4
65	Netblock	6
1	Netblock	2
65	Netblock	1
1	Netblock	1
65	Netblock	6
1	Netblock	6

Remove unselected entities from graph

Next >

Output - Transform Output

Transform To Netblock [Blocks delegated to this NS] returned with 12 entities (from entity "ans1.jcyl.q")
Transform To Netblock [Blocks delegated to this NS] returned with 12 entities (from entity "ans1.suw1")
Transform To Netblock [Blocks delegated to this NS] returned with 12 entities (from entity "ans1.nyc1")
Transform To Netblock [Blocks delegated to this NS] returned with 12 entities (from entity "ans1.sjc1")
Transform To Netblock [Blocks delegated to this NS] returned with 12 entities (from entity "ans1.dfw1")
Transform To Netblock [Blocks delegated to this NS] done (from 6 entities)

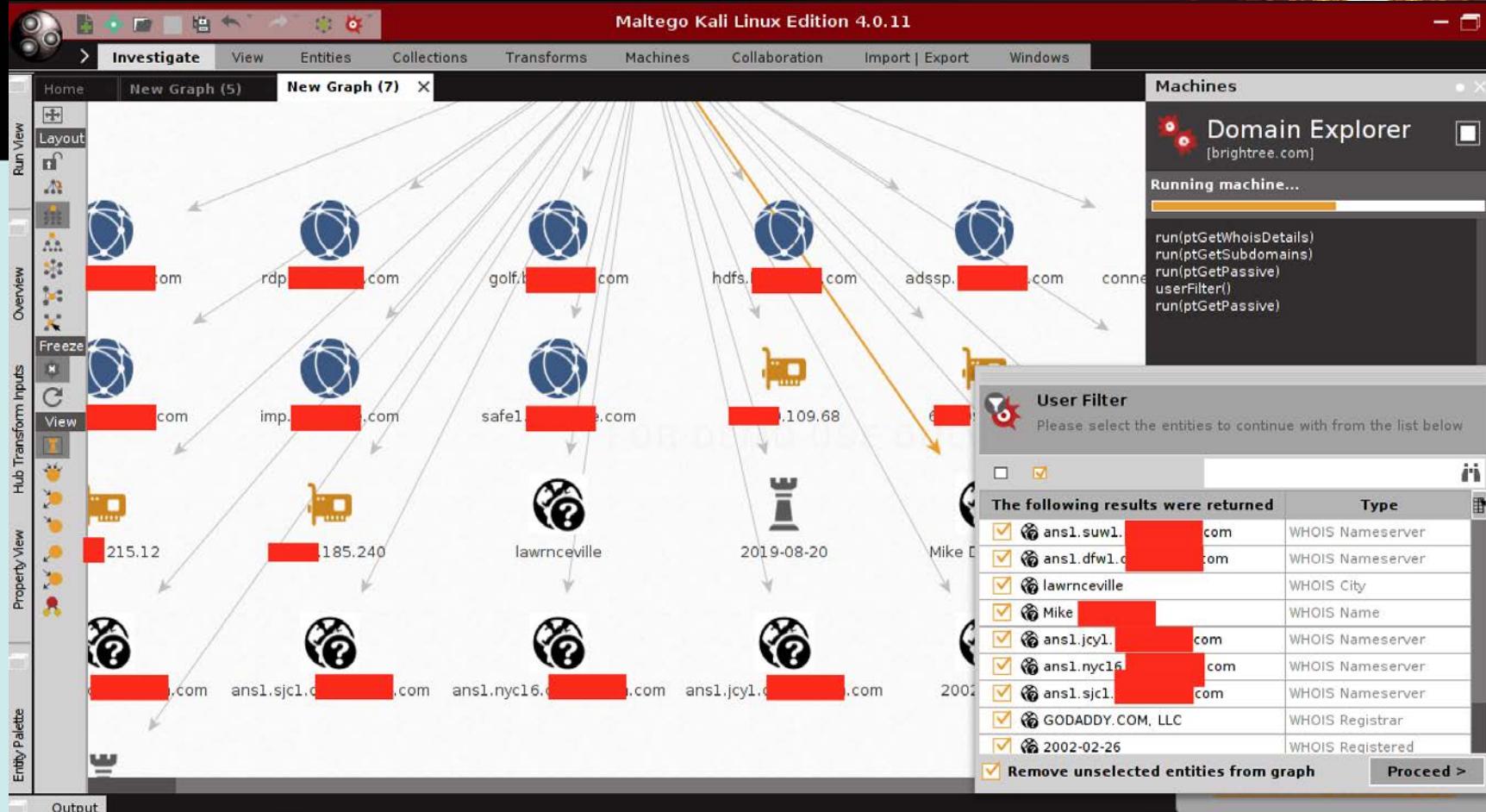
Footprint XXL

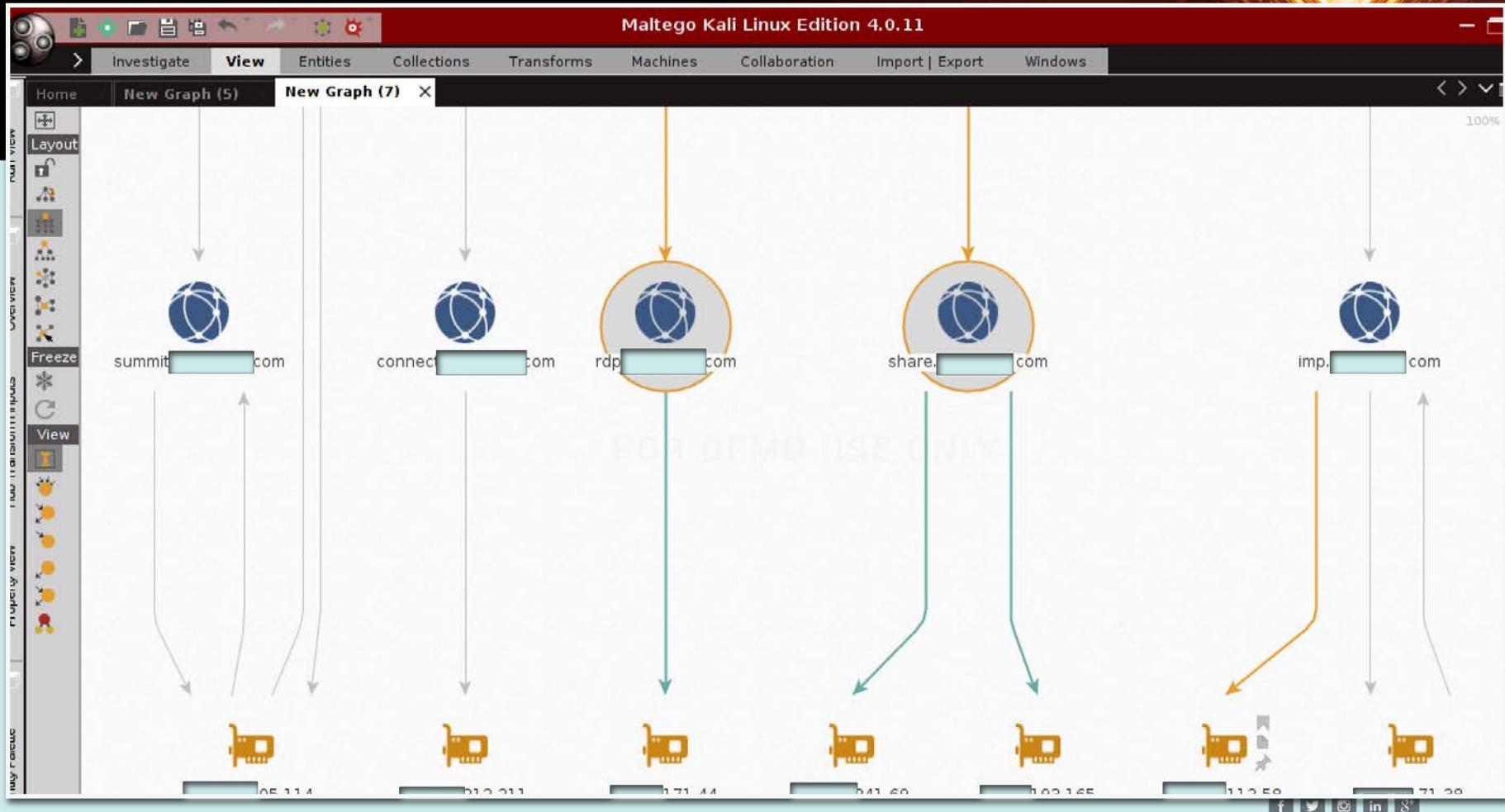
Running machine...

Function: domaininfo
userFilter(Choose relevant NS)
Deleted 7 entities
run(NSRecordToNetblock, NS4block)
userFilter(Select netblock)

Property ... Hub Tran... Over... >> X

25 entities, 80 links





NMAP

Zenmap

Scan Tools Profile Help

Target: rdp[REDACTED].com

Profile: Slow comprehensive scan

Scan Cancel

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" rdp[REDACTED].com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host	Port	Protocol	State	Service	Version
	share[REDACTED]	143	tcp	closed	imap	
	rdp[REDACTED].com	443	tcp	open	http	
		554	tcp	open	rtsp	
		587	tcp	closed	submission	
		993	tcp	closed	imaps	
		995	tcp	closed	pop3s	
		1433	tcp	open	ms-sql-s	Microsoft SQL Server 2008 R2
		1723	tcp	closed	pptp	
		3306	tcp	closed	mysql	
		3389	tcp	open	ms-wbt-server	
		5060	tcp	closed	sip	
		5666	tcp	open	nrpe	
		5800	tcp	closed	vnc-http	
		5900	tcp	closed	vnc	
		6000	tcp	closed	X11	
		7070	tcp	open	realserver	
		8080	tcp	closed	http-proxy	
		10000	tcp	open	ndmp	Symantec/Veritas Backup Exec ndmp (NDMPv3)

Filter Hosts

CYBERSECURITY READS
AN ISACA CYBER EVENT

f t in g+

5

[REDACTED].2.demo.hybris.com

, O=Let's Encrypt, CN=Let's Encrypt Authority X3
i441100ece8904ae728d609993a2469604d24a1ed523add81d780f451f2
xd Leaf Certificate

T=New South Wales, L=Sydney, O=[REDACTED] Inc., OU=IT, CN=store.[REDACTED].com
, L=Amsterdam, O=Verizon Enterprise Solutions, OU=Cybertrust, CN=Verizon Akamai SureServer CA G14-SH

f5a179d4bc445c2ec865585b4d16cfded149e7f26ba43ef9b6e154bef431
xd Leaf Certificate

d.subject.organization: [REDACTED] Inc.

T=Bavaria, L=Martinsried, O=[REDACTED] Germany Inc., CN=*.apuat.ccg.[REDACTED].com

, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
2cb129e8c2c7437b65e7f0884db8e5f847d8a03f0effa34f0d55c99e682d

xd Leaf Certificate

d.subject.organization: [REDACTED] Germany Inc.

T=California, L=San Diego, O=[REDACTED] Corp, CN=rms.[REDACTED].com

, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
046b20c54305795f285527165f888419f8abc273745578cf5b3d861f9b69

xd Leaf Certificate

d.subject.organization: [REDACTED] Corp

T=Bavaria, L=Martinsried, O=[REDACTED] Germany Inc., OU=IT Infrastructure Europe, CN=sslvpn.[REDACTED]

, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
5ee487d0d1622e2e6bd08ed1cc777c450a2a907302e2d6610344981c6f5c

xd Leaf Certificate

d.subject.organization: [REDACTED] Germany Inc.

T=Bavaria, L=Martinsried, O=[REDACTED] Germany Inc., OU=IT Infrastructure Europe, CN=sslvpn.[REDACTED]

, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
96dc3f712b0354cec2405475a1a240328955324b36b2e11d4dbc61449653

xd Leaf Certificate

d.subject.organization: [REDACTED] Germany Inc.

censys.io (semi-free)

- » Parsing and collection of various publically-available information
- » Example: certificates

- SSLVPN in France and Munich
- Date Center presence in Munich, San Diego, Sydney
- Demo-site of Hybrid (e-commerce technology)
- Using Akamai services in Sydney



censys.io - Geolocation

Secure https://www.censys.io/ipv4/[REDACTED]64.1

censys

[REDACTED]64.1

[REDACTED]64.1 (gw.[REDACTED].com.au)

Summary Details JSON WHOIS Raw WHOIS

Basic Information

Network [REDACTED]AS-SYD – [REDACTED] Dual Internet Gateway, AU (AU)
Routing [REDACTED]64.0/24 via AS [REDACTED]
Protocols no publicly accessible services

We haven't found any publicly accessible services on this host or the host is on our blacklist.

Map Satellite

Map data ©2017 GBRMPA, Google | Terms of Use

City [REDACTED]
Province New South Wales
Country Australia (AU)
Lat/Long [REDACTED]
Timezone Australia/Sydney

CISPA 2017
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

f t in g+

208.27.123.4

F

Added on 07.01.2014

USA Williamston

Details

Host IP: 208.27.123.4

[2][H]

***** Important Banner Message *****

Enable and Telnet **passwords** are configured to "**password**".

HTTP and HTTPS **default** username is "**admin**" and **password** is "**password**".

Please change them immediately.

The ethernet 0/1 interface is enabled with an address of 10.10.10.1

Telnet, HTTP, and HTTPS access are also enabled.

To remove this message, while in configuration mode type "no banner motd".

***** Important Banner Message *****

VIPs “Dorking”

Secure | <https://namechk.com>

Namech_k marco ermini

Domains

Help keep Namechk free [Donate PayPal](#) [Donate Bitcoins!](#)

.com	.net	.org	.co	.biz	.io	.ly	.us	.me	.co.uk	.eu	.info
.xyz	.ca	.be	.it	.am	.so	.tv	.la	.fr	.li	.ch	.ms
.jp	.at	.nu	.name	.pro	.work	.social	.guru	.help	.ninja	.bar	+

Click an *available* domain to purchase it. Click an *unavailable* domain to make an offer for it.

Usernames

[Download Results](#)

Facebook	YouTube	Twitter	Instagram	Blogger	GooglePlus	Twitch	Reddit	eBay	WordPress	Pinterest	Yelp
Slack	Github	Basecamp	Tumblr	Flickr	Pandora	ProductHunt	Steam	MySpace	Foursquare	OkCupid	Vimeo
UStream	Etsy	SoundCloud	BitBucket	Meetup	CashMe	Dailymotion	About.me	Discus	Medium	Behance	Photobucket

CSX 2017 EUROPE
CYBERSECURITY NEXUS
AN ISACA CYBER EVENT

[f](#) [t](#) [g](#) [in](#) [g+](#)

VIPs “Dorking”

Secure | <https://inteltechniques.com/OSINT/username.html>

INTEL TECHNIQUES .com

OSINT TRAINING & PRIVACY CONSULTING

Online Training Live Training Privacy Training Tools Forum Blog Podcast Books Bio Contact

Custom User Name Search

Populate All

KnowEm
NameVine
CheckUsers
Pipl
Pipl API
PeekYou
ThatsThem
UserSearch
Twitter
Facebook
YouTube
Tumblr
Instagram
Google +
Email

Pop-ups Submit All (Allow)

VIPs “Dorking”

The screenshot shows the Namevine website interface. At the top, there is a search bar with the URL <https://namevine.com/#/>. Below the search bar are navigation links for Search, About, Blog, and Feedback, along with a Settings icon.

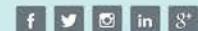
The main content area features a large banner with the text "Create A Consistent Online Presence" and "Instantly Find A Domain Name With Matching Social Media Profiles". Below the banner is a search input field with a placeholder and a clear button.

A section titled "Domains and Social Media Profiles" displays ten domain suggestions, each in a box with a status indicator (green for available, red for unavailable) and a "register" button:

- .COM is available! [register →](#)
- Twitter is available! [register →](#)
- Facebook is unavailable [view](#)
- Pinterest is available! [register →](#)
- YouTube is available! [register →](#)
- Instagram is available! [register →](#)
- Tumblr is available! [register →](#)
- Wordpress is available! [register →](#)
- Blogger is available! [register →](#)
- GitHub is available! [register →](#)

Below this section is a "Domain Suggestions" heading.

On the right side of the page, there are social sharing icons for Twitter, Facebook, Google+, and LinkedIn, along with a "Share" button.



VIPs “Dorking”

Secure | <https://www.facebook.com>

Marco Home 1

Message ...

Timeline About Friends Photos More ▾

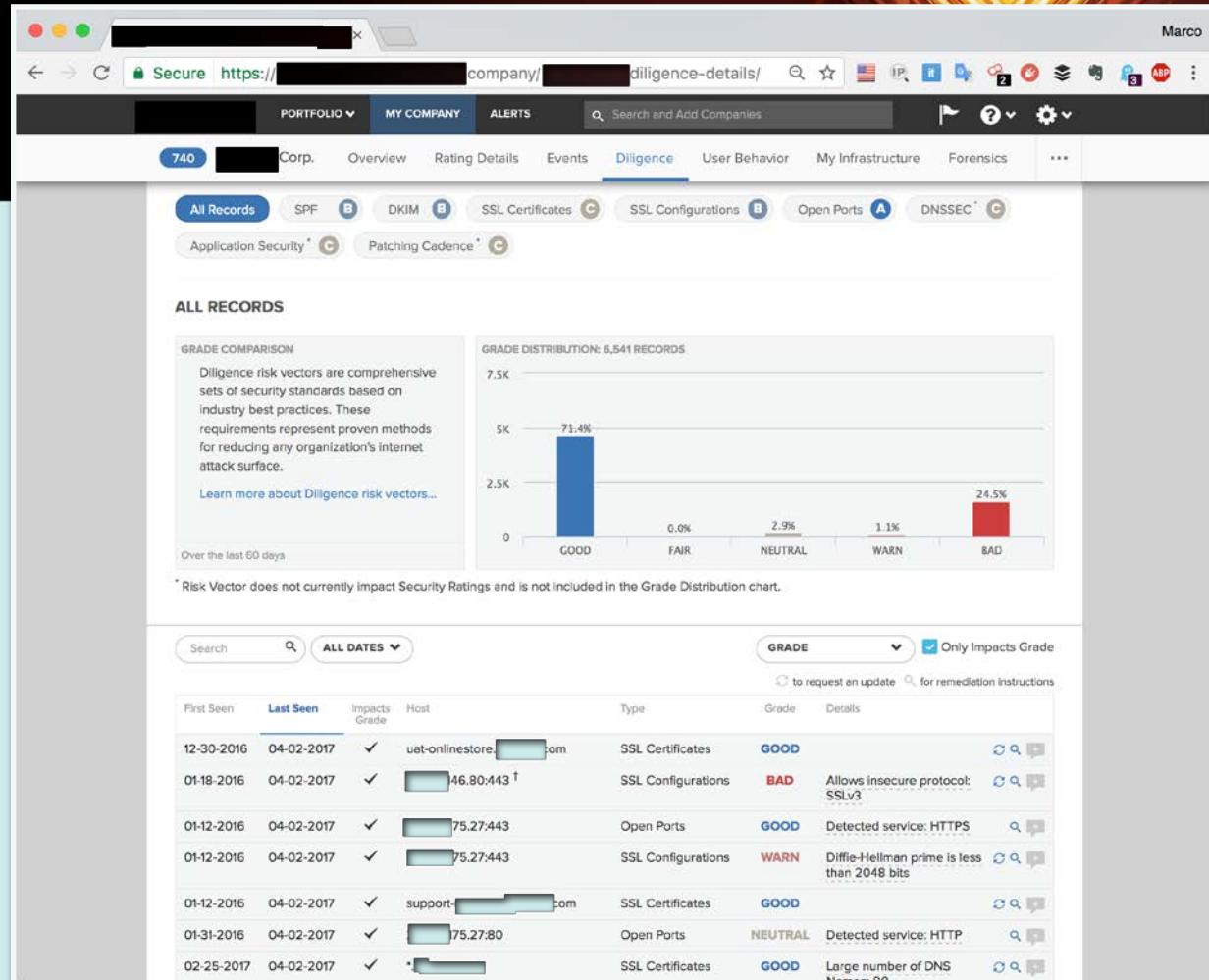
DO YOU KNOW [REDACTED]?

If you know [REDACTED] send him a message.

Photos Nothing to show

September 28, 2016 · YouTube · [REDACTED]

Great sounds. Thx Todd.



CyberSecurity Ratings Firms

03-30-2017	04-02-2017	✓	spf1.████████.com 2 PAST EVENTS ▾	SPF	WARN	Effective but allows a large number of hosts	
First Seen		Last Seen		Impacts Grade	Grade	Details	
03-24-2017		03-29-2017		✗	WARN	Effective but allows a large number of hosts	
06-06-2016		03-23-2017		✗	BAD	SPF record is ineffective	
03-30-2017	04-02-2017	✓	spf2.████████.com 3 PAST EVENTS ▾	SPF	WARN	Effective but allows a large number of hosts	
First Seen		Last Seen		Impacts Grade	Grade	Details	
03-24-2017		03-29-2017		✗	WARN	Effective but allows a large number of hosts	
08-20-2016		03-23-2017		✗	BAD	SPF record is ineffective	
06-06-2016		08-19-2016		✗	BAD	SPF record is ineffective	

Marco

Secure https://████████.com/company/████████/diligence-details/

PORTFOLIO ▾ MY COMPANY ALERTS Search and Add Companies

740 ██████████ Corp. Overview Rating Details Events Diligence User Behavior My Infrastructure Forensics

LAST 60 DAYS

Port	Total Hosts	Grade Distribution	Service
21	5	<div style="width: 80%; background-color: #0070C0;"></div>	Detected service: FTP with STARTTLS and 1 other service
22	17	<div style="width: 90%; background-color: #0070C0;"></div>	Detected service: SSH and 1 other service
25	6	<div style="width: 60%; background-color: #0070C0;"></div> <div style="width: 20%; background-color: #A52A2A;"></div>	Detected service: SMTP without STARTTLS and 2 other services

PORT 137 – REPRESENTATIVE EVENTS

LAST 60 DAYS – 1 HOST

First Seen	Last Seen	Host	Grade	Details
12-29-2016	03-30-2017	████████.137	BAD	Detected service: NetBIOS

EVENTS OLDER THAN 60 DAYS – 1 HOST
These events do not impact this company's current Open Ports letter grade.

First Seen	Last Seen	Host	Grade	Details
01-13-2016	06-14-2016	████████.137	BAD	Detected service: NetBIOS

ISSUE REMEDIATION INSTRUCTIONS

Detected service: NetBIOS Block the port on company edge network infrastructure, as well as within the machine itself, and ensure the machine receives a thorough administrative security review. If NetBIOS connectivity is required, tunnel any connections through a

OPEN PORT DETAILS FOR
████████:137
Observed on Mar 30, 2017 at 21:33

MAC address: ██████████
Server Name: ██████████

Port	Total Hosts	Grade Distribution	Service
465	3	<div style="width: 80%; background-color: #0070C0;"></div>	Detected service: SMTPS
500	17	<div style="width: 90%; background-color: #0070C0;"></div>	Detected service: ISAKMP and 1 other service
587	1	<div style="width: 90%; background-color: #0070C0;"></div>	Detected service: SMTP with STARTTLS
636	1	<div style="width: 90%; background-color: #0070C0;"></div>	Detected service: HTTPS
993	5	<div style="width: 80%; background-color: #0070C0;"></div>	Detected service: IMAPS

Show results 1 to 20 of 22 entries

CyberSecurity Ratings Firms

PORT 123 – REPRESENTATIVE EVENTS

LAST 60 DAYS – 33 HOSTS

First Seen	Last Seen	Host	Grade	Details
03-24-2017	04-02-2017	[REDACTED] 246.204:123	NEUTRAL	Detected service: NTP
04-02-2017	04-02-2017	[REDACTED] 64.1:123	NEUTRAL	Detected service: NTP
04-02-2017	04-02-2017	[REDACTED] 76.1:123	NEUTRAL	Detected service: NTP
04-02-2017	04-02-2017	[REDACTED] 76.3:123	NEUTRAL	Detected service: NTP
03-28-2017	04-02-2017	[REDACTED] 83.1:123	NEUTRAL	Detected service: NTP
03-25-2017	04-02-2017	[REDACTED] 147.255:123	NEUTRAL	Detected service: NTP
04-01-2017	04-02-2017	[REDACTED] 84.254:123	NEUTRAL	Detected service: NTP

X OPEN PORT DETAILS FOR [REDACTED] 246.204:123
Observed on Apr 2, 2017 at 23:40

i Product: ntpd
i Version: 4
i Data:

```
ntp
version: 4
processor: unknown
system: UNIX
leap: 0
stratum: 3
precision: -10
rootdelay: 34.245
rootdispersion: 56.347
peer: 48614
refid: [REDACTED] 6.133
reftime: 0xdc8c096f.920689d4
poll: 10
clock: 0xdc8c09fc.9166e454
```

Marco

Secure https://[REDACTED].com/company/[REDACTED]/event-evidence/

PORTFOLIO ▾ MY COMPANY ALERTS Search and Add Companies

740 [REDACTED] Corp. Overview Rating Details Events Diligence User Behavior My Infrastructure Forensics ...

FORENSICS Download forensics data

FILTER Showing events 1–2 of 2. Order results by: MOST RECENT ▾

IP ADDRESS SEARCH e.g. 192.0.2.0

TIME RANGE All Time Date Seen: 05-07-2016

Last 7 days

Last 30 days

Custom Date Range

NARROW BY RISK VECTOR

Events

Botnet Infections (2)

Spam Propagation (0)

Malware Servers (0)

Potentially Exploited (7)

Unsolicited Comm. (0)

User Behavior PREMIUM

Botnet Infections: Zeus

Source Port: 17776
Destination Port: 80
Server Name: xdqzpbgrvjk.ru
Details ▾

IP Address: 246.156

Botnet Infections: Gamarue

Source Port: 37059
Destination Port: 80
Server Name: somicrosoft.ru
C&C IP: XXX.22.28.198
Observations: 208
Request Method: POST
First Seen: 2016-05-07 15:21:31 UTC
Last Seen: 2016-05-07 19:23:01 UTC
Representative Event Timestamp: 2016-05-07 15:21:31 UTC
User Agent: Mozilla/4.0
Details ▾

IP Address: 246.156

FILTER BY INFECTIONS

Zeus (1)

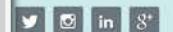
Gamarue (1)

NARROW BY TAGS

Sx 2017
EUROPE

SECURITY NEXUS

ITALIA CYBER EVENT



Data Breaches

Secure | <https://www.forbes.com/sites/leemathews/2017/03/15/donald-trump-expo...> ☆ 2

Security / #CyberSecurity

MAR 15, 2017 @ 02:00 PM 2,797 ◊

The Little Black Book of Billionaire Secrets

Donald Trump Exposed Among 33M Records In Massive New Database Leak



Lee Mathews, CONTRIBUTOR
Observing, pondering, and writing about tech. Generally in that order. [FULL BIO](#) ▾
Opinions expressed by Forbes Contributors are their own.

Researchers have discovered yet another massive cache of private data that was exposed online. This particular database was a whopping 52.2 gigabytes in size, and it included contact information and organizational structures of thousands of U.S. businesses and agencies.



Datacenter image courtesy Pexels

Troy Hunt, the security researcher who I spoke with

Cyber

RISK VECTOR BREAKDOWN

EVENTS

- Botnet Infections B
- Spam Propagation A
- Malware Servers A
- Unsolicited Communication A
- Potentially Exploited B

DILIGENCE

- SPF Domains B
- DKIM Records B
- TLS/SSL Certificates C
- TLS/SSL Configurations B
- Open Ports A
- DNSSEC Records * C
- Application Security * C
- Patching Cadence * C

USER BEHAVIOR

- File Sharing C
- Disclosed Credentials N/A

OTHER

- Data Breaches A

DISCLOSED CREDENTIALS



34

BREACHES

2,752

TOTAL RECORDS

The Disclosed Credentials risk vector indicates whether employees of a company have had their personal or corporate information disclosed as a result of a publicly disclosed data breach. Disclosed Credentials is an informational risk vector and will never affect a company's Security Rating. Many websites do not validate email addresses, which makes it difficult to assert that certain exposed records are associated with a company's employees. Likewise, BitSight does not test that disclosed credentials are valid, for example by trying a username and password disclosed from a breached site, in order to preserve business confidence and trust. [Read more...](#)

Date	Breached Site	Domain	Record(s)
2017-Jan-01	River City Media Spam List	.com and 4 more	113 🔍
2017-Jan-01	CloudPets	.com	1 🔍
2016-Dec-05	MrExcel	.com and 1 more	6 🔍
2016-Oct-08	Modern Business Solutions	.com and 1 more	3 🔍
2016-Sep-10	Leet	.com and 1 more	5 🔍
2016-Sep-01	NetProspect	.com and 7 more	1,132 🔍
2016-Aug-07	Wishbone	.com	1 🔍

FIRST

PREVIOUS

1

2

3

...

5

NEXT

LAST

X-2017-EUROPE
CYBER EVENT

NETPROSPEX - 2016-SEP-01

Description

In 2016, a list of over 33 million individuals in corporate America sourced from Dun & Bradstreet's NetProspx service was leaked online. D&B believe the targeted marketing data was lost by a customer who purchased it from them. It contained extensive personal and corporate information including names, email addresses, job titles and general information about the employer.

Disclosed Attributes

Email Addresses, Name, Phone numbers, Physical Address

Domain(s)	Record(s)
.com	845
.com	204
.com	44
.com	11
.net	7
.com	7
.com	7
.com	7

Your security posture is *good* in your industry.



Sample Company Inc.

Sample Industry

sample-company-inc.com

WHAT DOES THIS SCORE MEAN?

Your security posture score is based on your grades across ten major security categories.

Let's check the areas where your company could use improvement.

Note: This is a limited view.

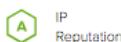
CLICK A CATEGORY TO LEARN MORE



Application Security



DNS Health



IP Reputation



Network Security



Patching Cadence



Social Engineering



Endpoint Security



Information Leak



Hacker Chatter



Cubit Score

Web Application Security

YOUR SCORE

ISSUES FOUND



1

Web apps are the engine of the online experience. Boasting cloud storage and dynamic use, web apps have become a part of daily life as people increasingly rely on them for business, productivity, and entertainment.

[How web apps get exploited >](#)

DNS Health

YOUR SCORE

ISSUES FOUND



0

DNS health is all about the quality and authenticity of the emails that fill your inbox. The Domain Name System (DNS) is critical for identifying mail exchange servers. It is also how we do attribution via email addresses, and not obscure IP addresses.

[Why email security matters >](#)

IP Reputation

YOUR SCORE

ISSUES FOUND

Network Security

YOUR SCORE

ISSUES FOUND

Secure | https://demo.com/enterprise/dashboard/all

DASHBOARD ASSESSMENTS VENDORS REPORTS USERS COMPANY PROFILE

Dashboard

All Portfolio Risk Metrics

Vendor Ratings: 49 Vendors

Rating	Count
Weak	1
Fair	2
Good	1
Excellent	46

Average iTrust Rating: 5004

Date	iTrust Rating
Sep 23 2016	4500
Oct 21 2016	4500
Nov 18 2016	4500
Dec 16 2016	4500
Jan 13 2017	4500
Feb 10 2017	4500
Mar 31 2017	6500
Apr 28 2017	6000

Highest Risk Vendors

Vendor	Contact	iTrust Rating	Status
Company_19	lulurikuzi@car101.pro	1000	Active
Company_14	jopoyamaw@go2usa.info	1000	Active
Company_10	linozaz@loan101.pro	1000	Active
Company_25	xowubem@go2usa.info	1789	Active
Company_50	testcomp0003@gmail.com	2153	Active

Vendor Compliance Status

Compliance Framework: [dropdown menu]

Vendor Compliance Aging

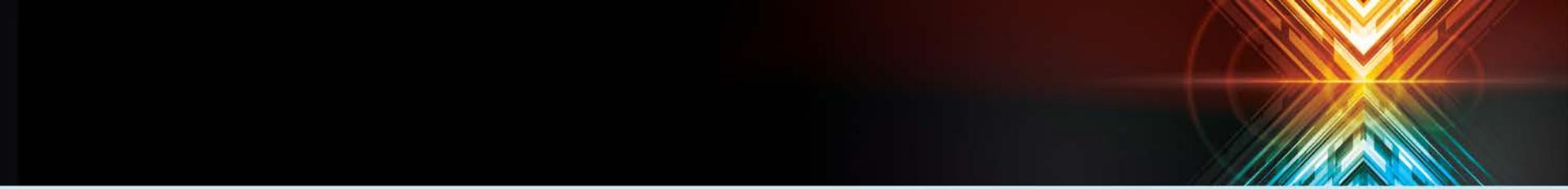
69% + - 1:1

f t in g+

Bibliography

- » "Mergers and Acquisitions Security – Corporate Restructuring and Security Management" (E.P. Halibozek, Dr. G.L. Kovacich), Elsevier, 2005
- » "Information Security in Mergers & Acquisitions" (C. Conacher), Black Hat 2004
- » "Handling mergers and acquisitions: Career success tips for infosec pros", searchsecurity.techtarget.com
- » "Using Open Source Reconnaissance Tools for Business Partner Vulnerability Assessment" (SANS Institute InfoSec Reading Room), 2014
- » "Why people integration continues to dominate M&A challenges", PWC, 2012
- » "Plan and Execute an Active Directory Merger", windowsitpro.com, 2009
- » "The Three Steps to Consolidate the Active Directory Environments of Merging Organizations", binarytree.com, 2015
- » "Collaborations, mergers, acquisitions, and security policy conflict analysis" (V. Subramanian, R. Seker, J. Bian, N. Kanaskar, acm.org, 2011)
- » "Alignment of the IS Organization: the Special Case of Corporate Acquisitions" (C.V. Brown, J.S. Renwick), 1996
- » "M&A loves the cloud", "M&A Trends", Deloitte, 2016
- » "Driving growth and competitiveness: Can the power of cloud lift M&A value into the stratosphere?", Accenture, 2016
- » "Lifecycle of a Technology Company – Step-by-step legal background and practical guide from start-up to sale", E.L. Miller Jr., John Wiley & Sons, 2008
- » "Mergers and Acquisitions from A to Z" 3rd ed., A.J. Sherman, AMACOM, 2011
- » "Digging for Disclosure – Tactics for Protecting Your Firm's Assets from Swindlers, Scammers, and Imposters", K.S. Springer and J. Scott, Pearson Education, 2011
- » "Mergers & Acquisitions For Dummies Cheat Sheet" – dummies.com
- » "The Complete Guide to Mergers & Acquisitions: Process Tools to Support M & A Integration at Every Level, Third Edition" T.J. Galpin, Wiley, 2014





THANK YOU!

Marco Ermini
2017

