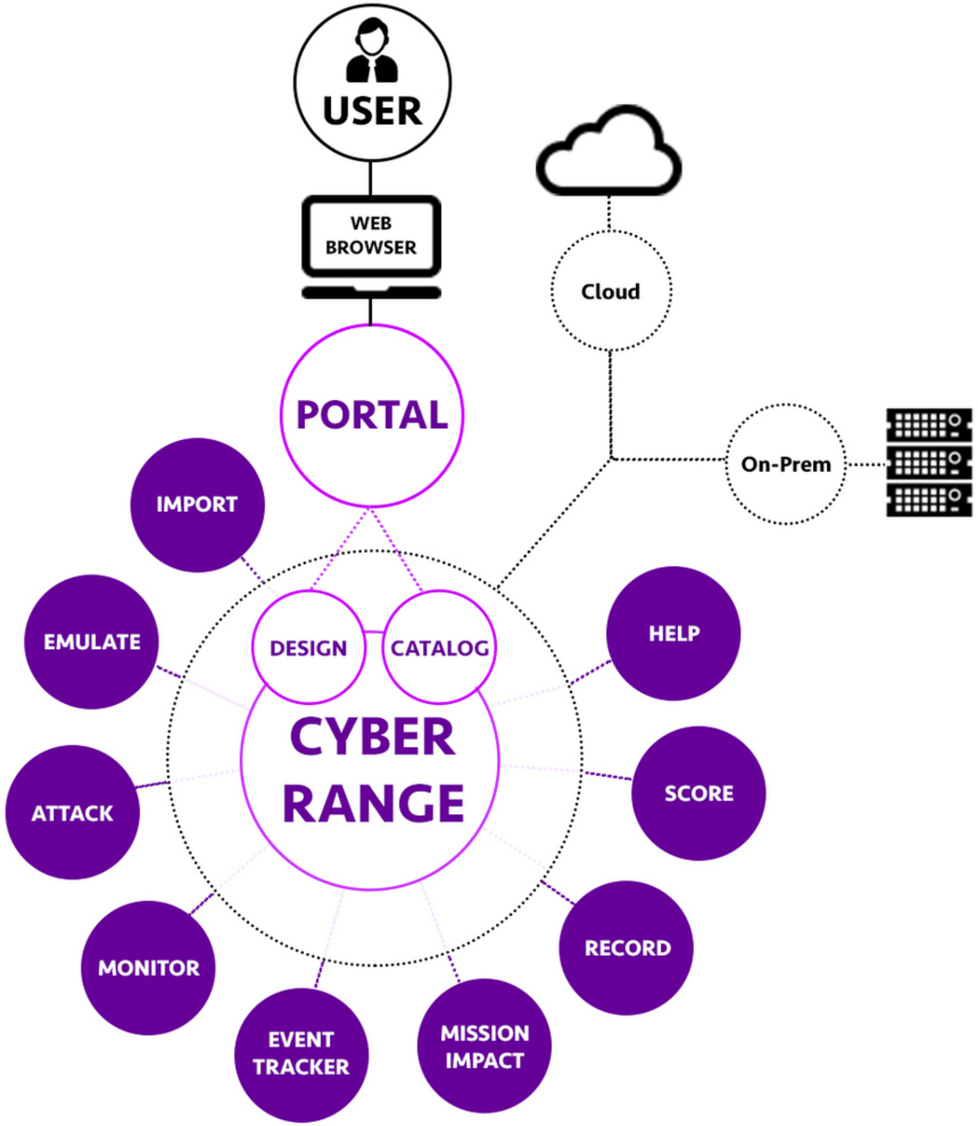
SIMSPACE CORPORATION

SimSpace Cyber Range

SimSpace

BOSTON (HQ)
51 Melcher St.
Boston, MA 02210
www.simspace.com

THE SIMSPACE CYBER RANGE



Make complex and laborious network environments simple to create and provide accessible, affordable, and sophisticated solutions to meet your cybersecurity research, development, testing, and training needs

Required Elements for Network Cloning

Unique business systems

Network security

Network discovery

Users

Applications

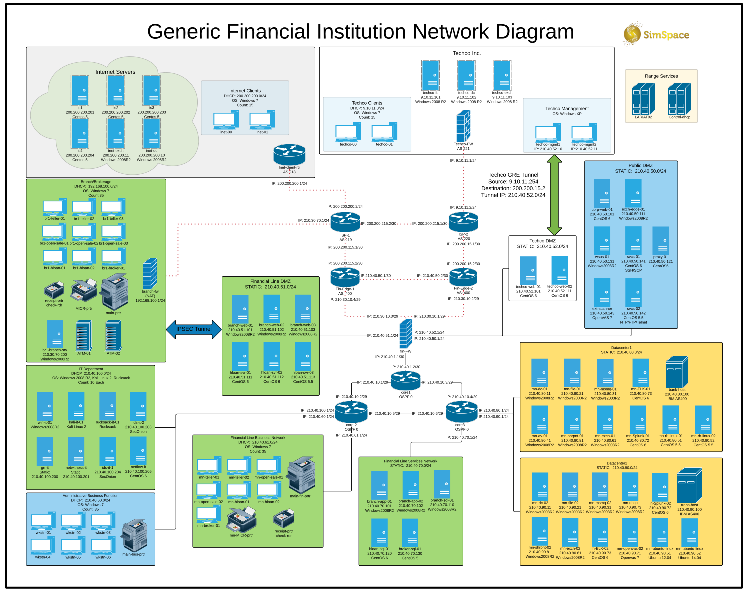
Internet sites & services

Services

Active Directory

Infrastructure

Operating Systems



Many components must be installed and configured like the real network; fully automated build process

Cyber Range Hosting

Cloud-Based

- Range-as-a-service
- Hosted in public cloud (AWS, Google)
- Isolated environment
- Nearly unlimited capacity
- Rapid updates

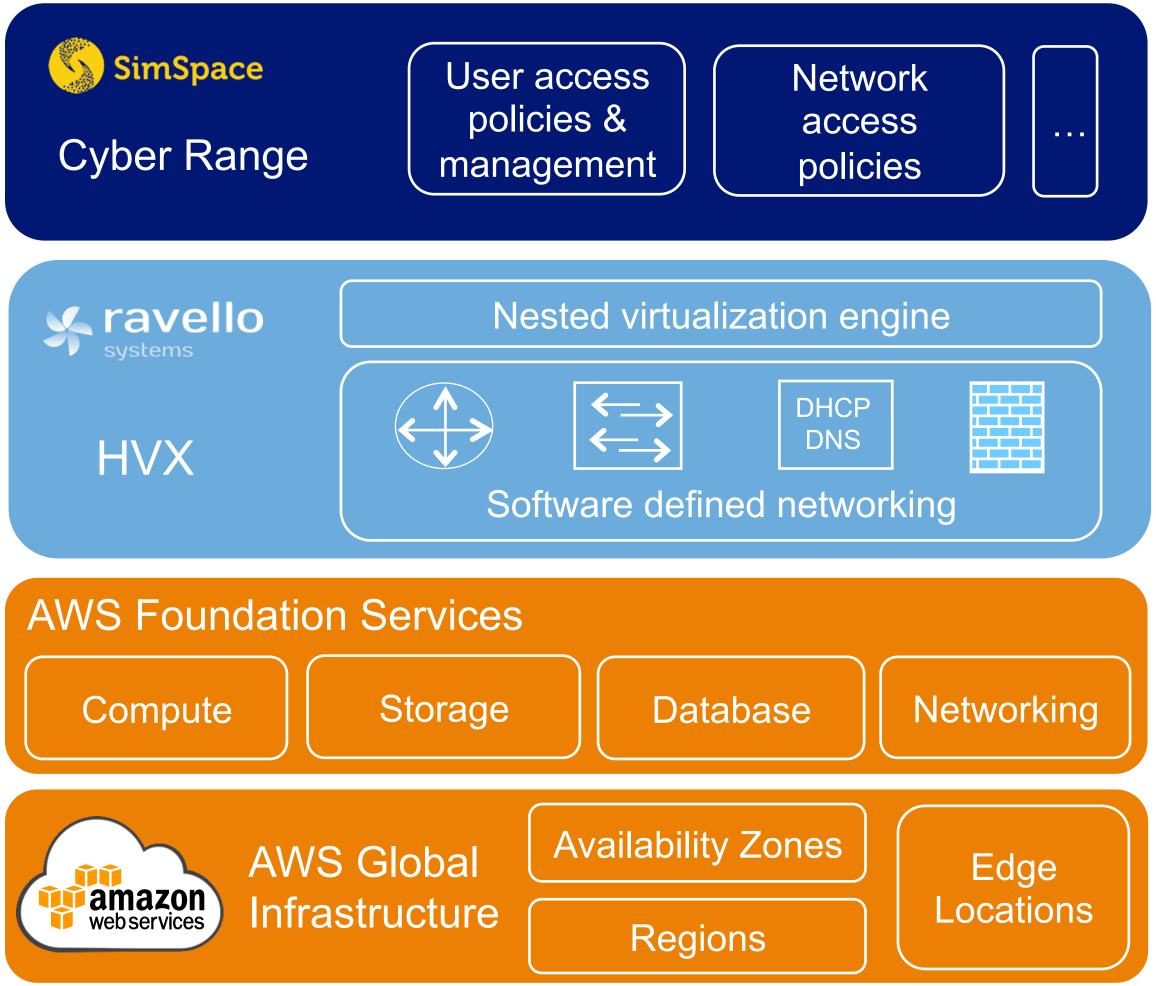
SimSpace Hosted

- Range-as-a-service
- Hosted at SimSpace datacenter
- Isolated environment
- Increased data assurances
- Rapid updates
- Inclusion of physical devices

Enterprise

- Hosted on-premises
- Tied into existing infrastructure
- Controlled access, data and results
- Integrate with physical devices
- Integrate with internal systems

Cloud Components & Security



Centrally manage users, access policies, networks, test/training results and security controls

High performance nested virtualization and overlay network

Secure capsule. Isolated self-contained environments – prevent leakage into cloud

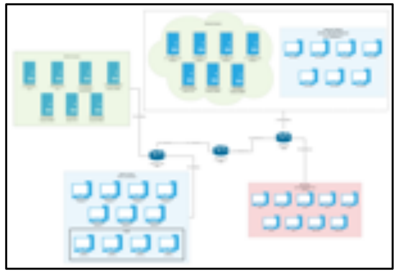
Catalog: Preconfigured Networks

Mini-network

Size: 15 hosts
Difficulty: -

- Internet emulation
- Mini network enclave

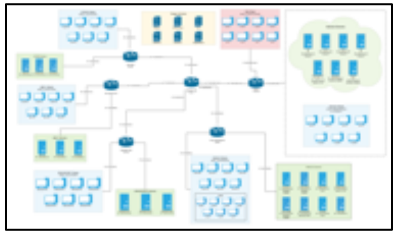
Generic Small



Size: 40 hosts
Difficulty: -

- Internet emulation
- 1 Simple network
- Red Team hosts

Generic Medium



Size: 80 hosts
Difficulty: 0.91

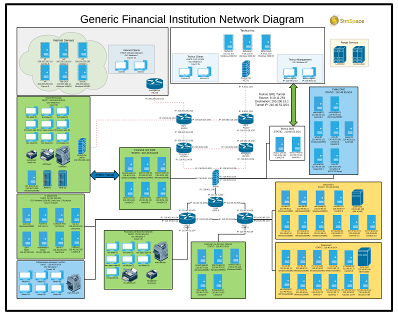
- Internet emulation
- 4 Simple networks
- Red Team hosts

Military

Size: 150 hosts
Difficulty: 1.26

- Internet emulation
- Island defense
- Tri-service network
- Military critical system

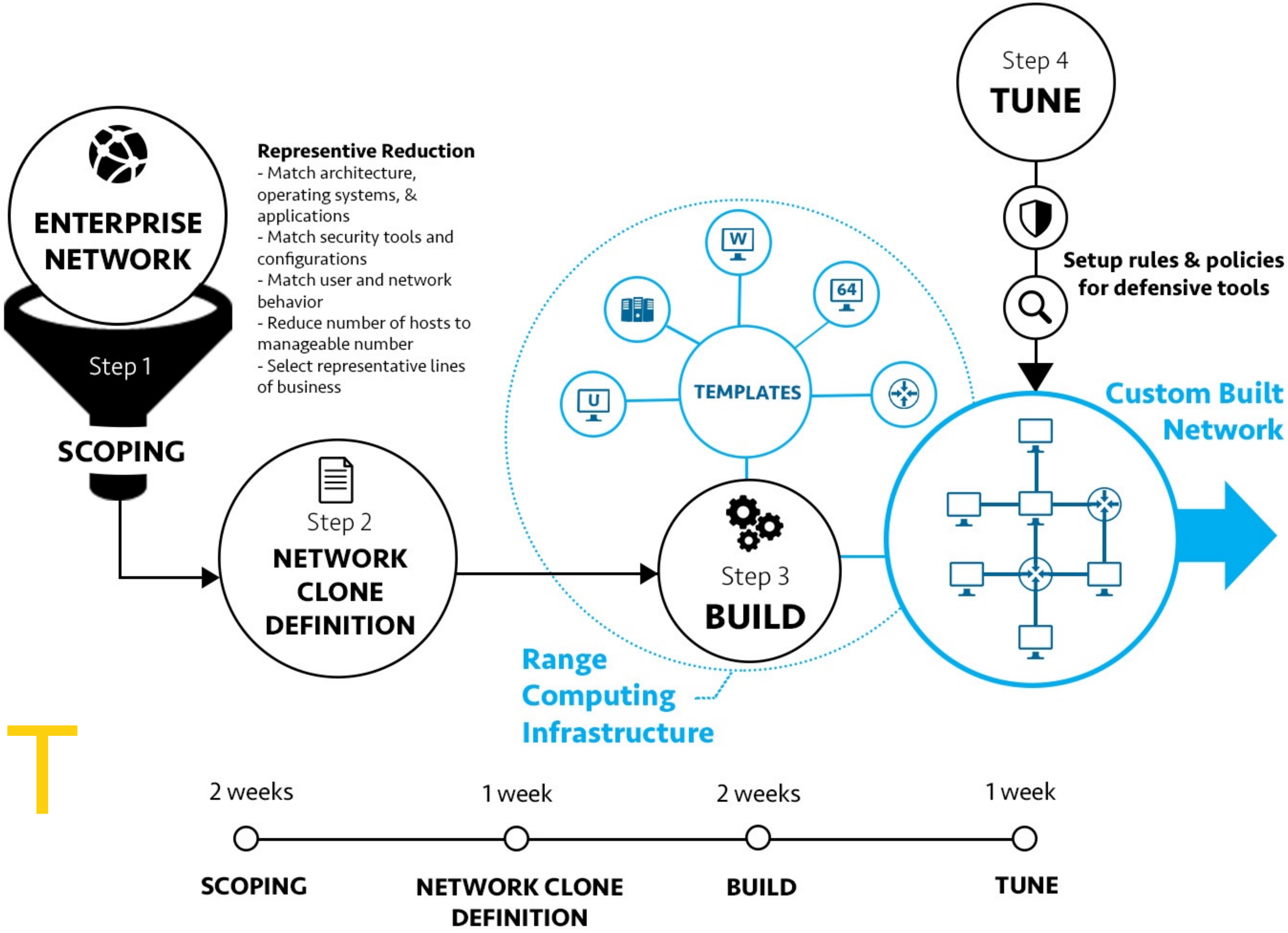
Generic Financial



Size: 280 hosts
Difficulty: -

- Internet emulation
- Financial business units
- Core financial services
- 3rd Party network

RANGE BUILDOUT



ENTERPRISE NETWORK

Step 1

SCOPING

Representive Reduction
- Match architecture, operating systems, & applications
- Match security tools and configurations
- Match user and network behavior
- Reduce number of hosts to manageable number
- Select representative lines of business

Step 2

NETWORK CLONE DEFINITION

TEMPLATES

Step 3

BUILD

Range Computing Infrastructure

Step 4

TUNE

Setup rules & policies for defensive tools

Custom Built Network

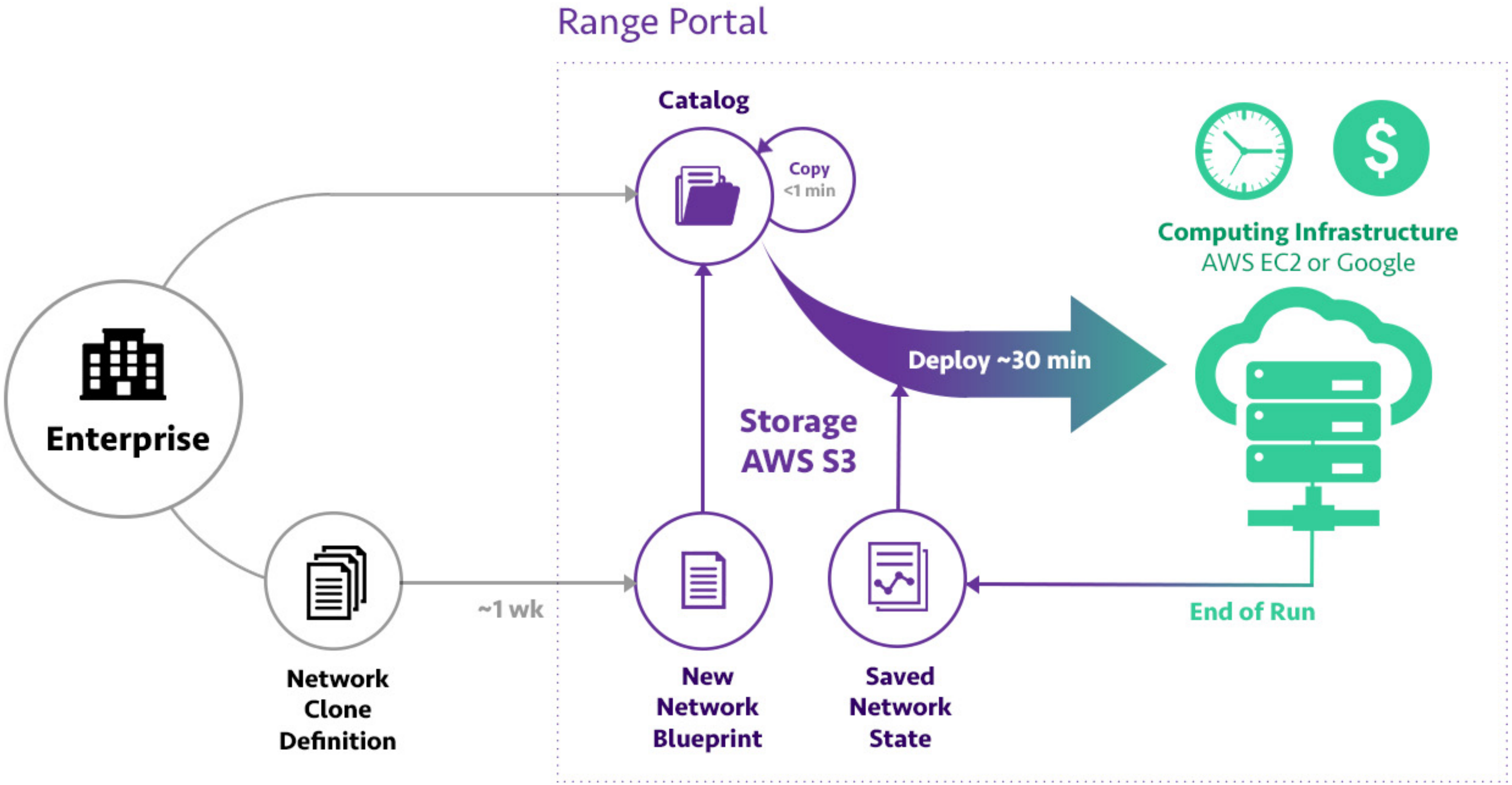
2 weeks — SCOPING

1 week — NETWORK CLONE DEFINITION

2 weeks — BUILD

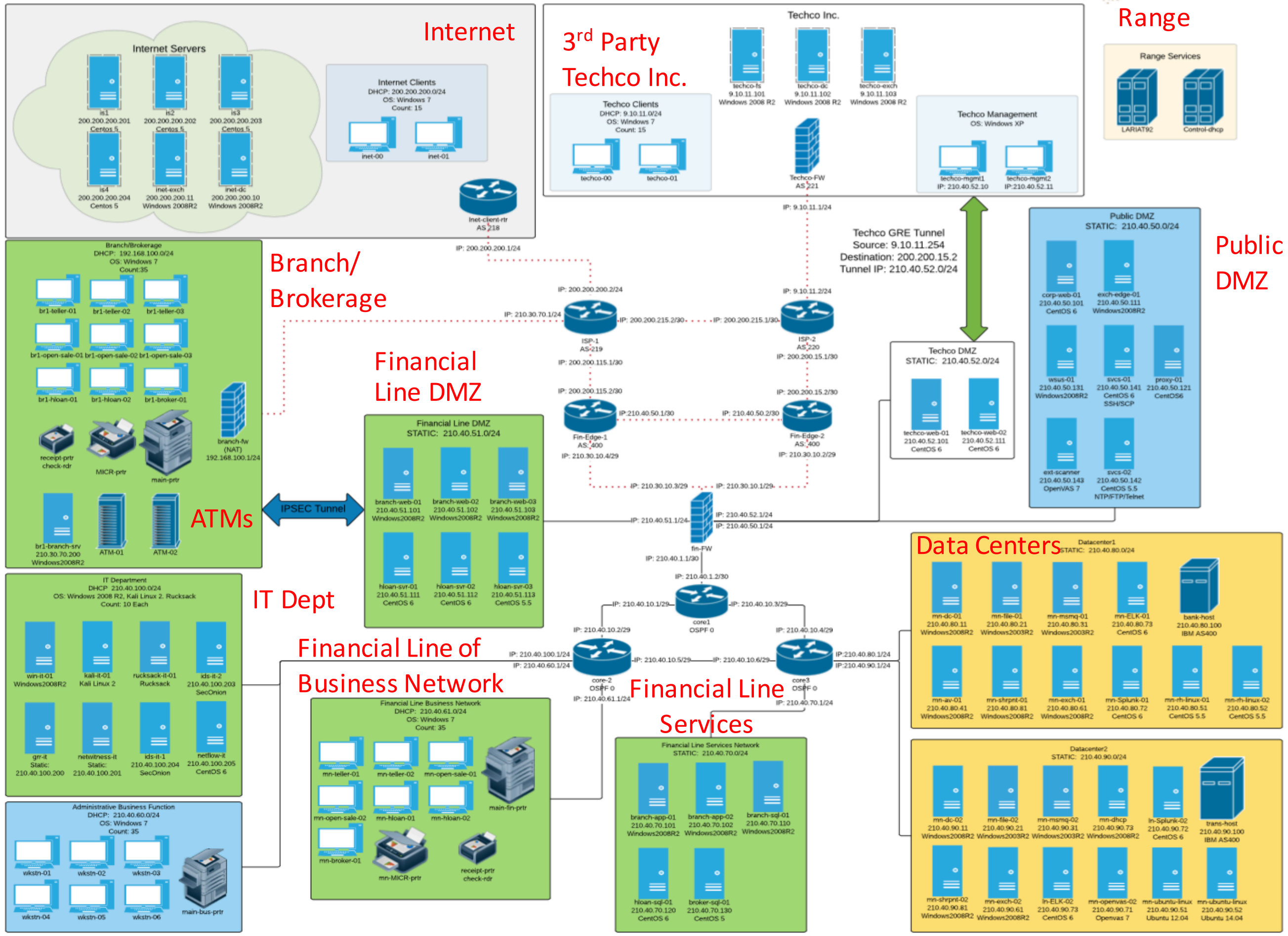
1 week — TUNE

Cloud-Based Cyber Range



- Creation of new network blueprints: up to 30 mins
- Time to copy blueprint: less than 1 min
- Number of network blueprints and variations (e.g. A/B testing, individual networks per team): nearly unlimited (AWS S3)
- Time to deploy range to computing infrastructure: up to 30 mins
- Range costs: only pay for range use (execution time) not infrastructure or number of copies
- No user scheduling or resource allocation concerns

Generic Financial Network Overlay


Internet
Internet Servers
Internet Clients
inet-clent-rtr
3rd Party Techco Inc.
Techco Inc.
Techco Clients
Techco-FW
Techco Management
Range
Range Services
LARIAT92
Control-dhcp
Techco GRE Tunnel
Source: 9.10.11.254
Destination: 200.200.15.2
Tunnel IP: 210.40.52.0/24
Public DMZ
Public DMZ STATIC: 210.40.50.0/24
Techco DMZ STATIC: 210.40.52.0/24
Branch/ Brokerage
Branch/Brokerage DHCP: 192.168.100.0/24 OS: Windows 7 Count:35
ISP-1
ISP-2
Fin-Edge-1
Fin-Edge-2
Financial Line DMZ
Financial Line DMZ STATIC: 210.40.51.0/24
ATMs
ATM-01
ATM-02
IPSEC Tunnel
fin-FW
core1 OSPF 0
core-2 OSPF 0
core3 OSPF 0
IT Dept
IT Department DHCP: 210.40.100.0/24 OS: Windows 2008 R2, Kali Linux 2, Rucksack Count: 10 Each
Financial Line of Business Network
Financial Line Business Network DHCP: 210.40.61.0/24 OS: Windows 7 Count: 35
Administrative Business Function DHCP: 210.40.60.0/24 OS: Windows 7 Count: 35
Financial Line Services
Financial Line Services Network STATIC: 210.40.70.0/24
Data Centers
Datacenter1 STATIC: 210.40.80.0/24
Datacenter2 STATIC: 210.40.90.0/24

General

- 280 nodes
- 15 span ports

Operating Systems

- Windows 2008 R2,
- Windows 7
- CentOS, Ubuntu, Kali

Applications

- MS Office,
- IE, Chrome, Firefox
- Active Directory, Exchange
- IIS, Apache

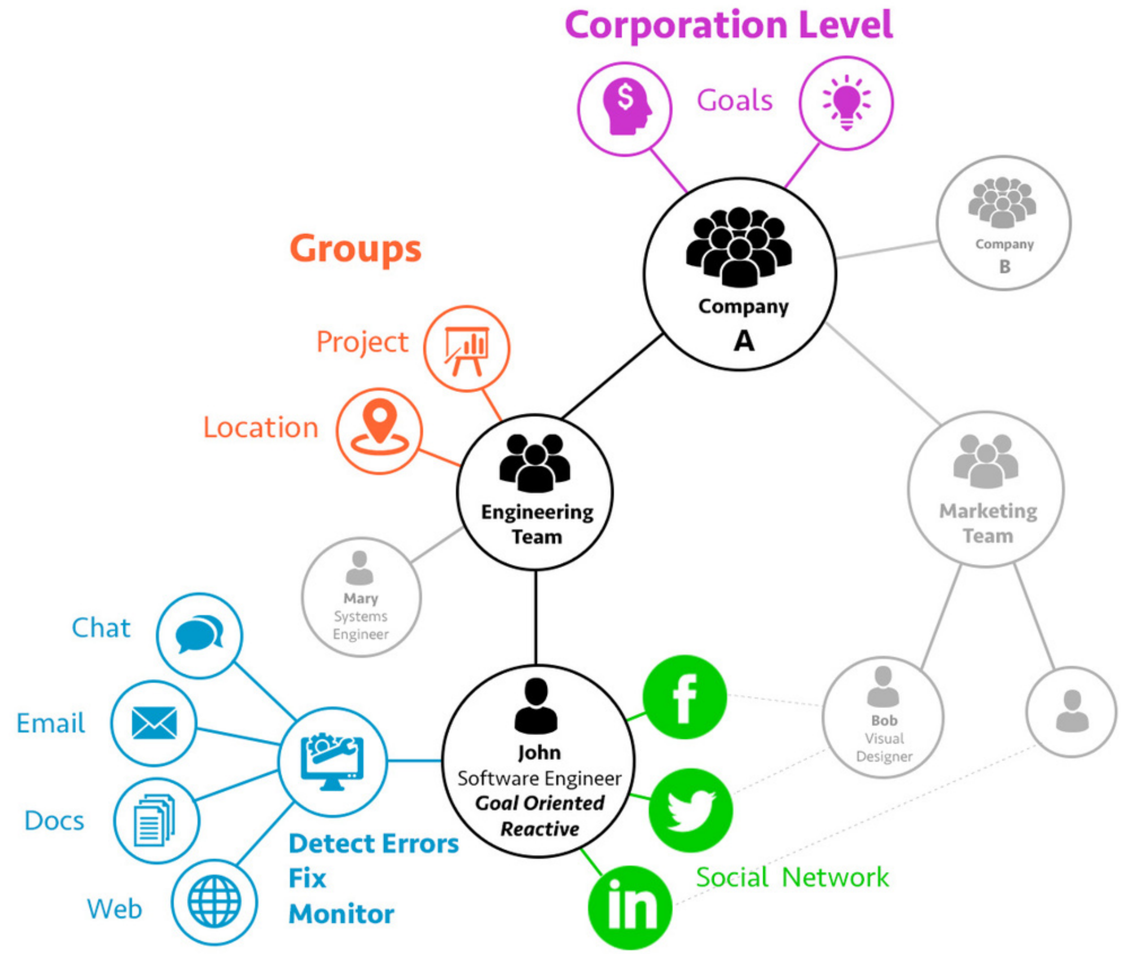
Security Tools

- Symantec SEP
- Splunk, Tanium, Qualys
- RSA Netwitness
- Security Onion
- ELK, GRR

Network Instances

- Copies for team training
- Copies for new products (A/B testing)

Enterprise User Emulation

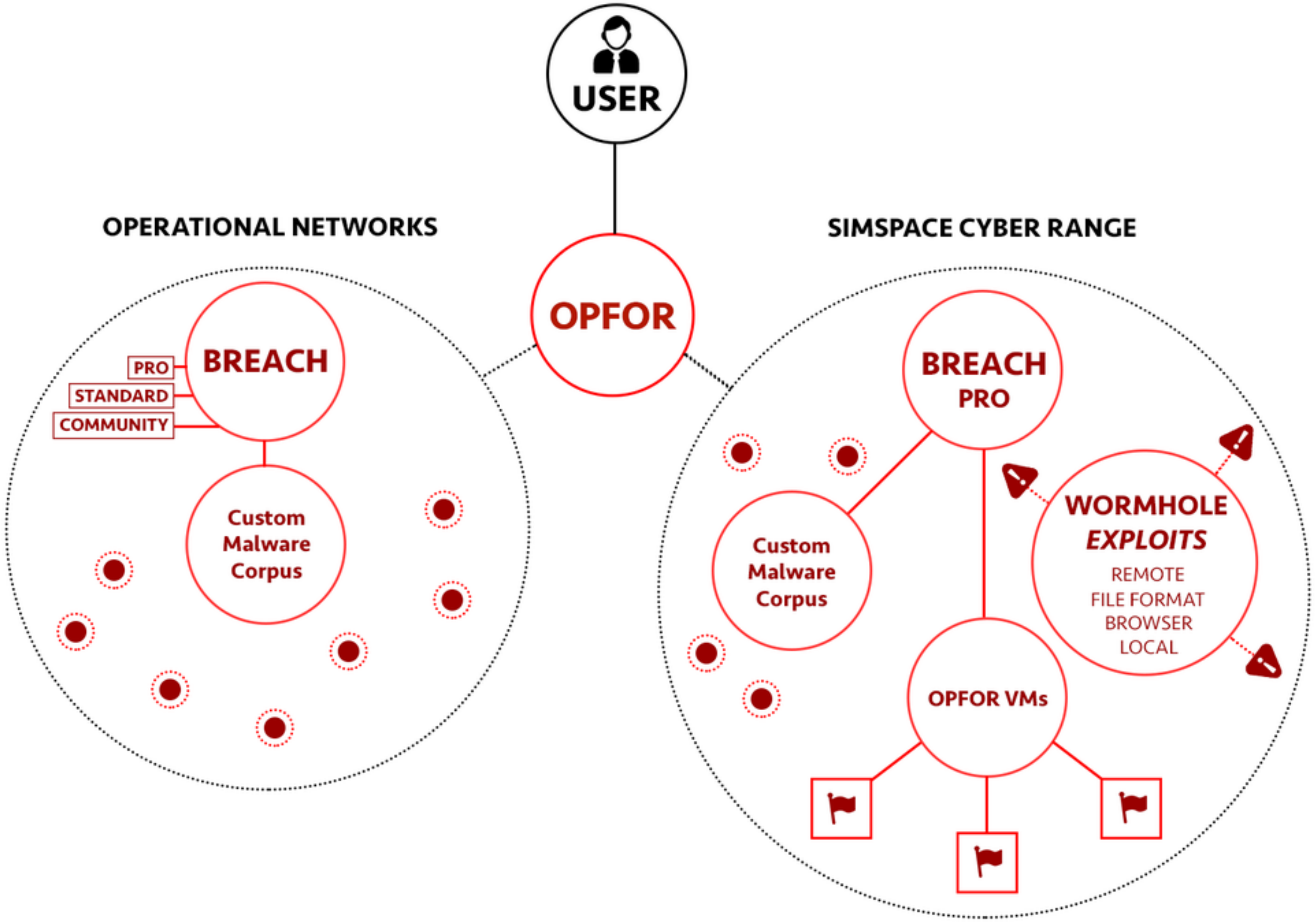


Traffic generation via intelligent host-based agents to accurately emulate enterprise activity

VIRTUAL USERS

- Unique personas with their own accounts, documents, user behaviors, application biases, social groups, projects
- Interact with real applications on each host (e.g. MS Office, IE, Firefox) like a typical user
- Collaborate with other users to accomplish broader tasks
- Can scale to thousands of users across platform types
- Generate realistic workload on each host & network
- Create means for attackers to exploit clients & hide in enterprise traffic

Attack Tools



Attack tools to simulate sophisticated attacks, APT1, CyberSnake, etc...

Run attack scenarios automatically by combining discrete attacker tasks to form a full attack

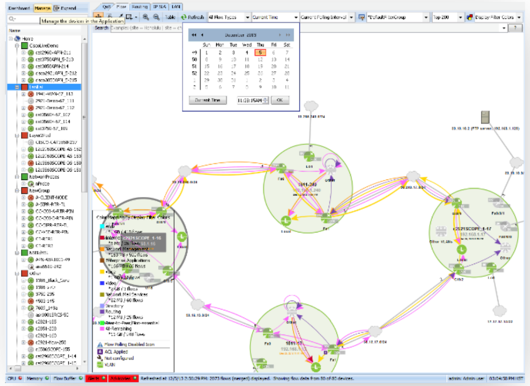
Custom malware exercising blue’s ability to identify and contain malware communications and persistence utilizing all common techniques

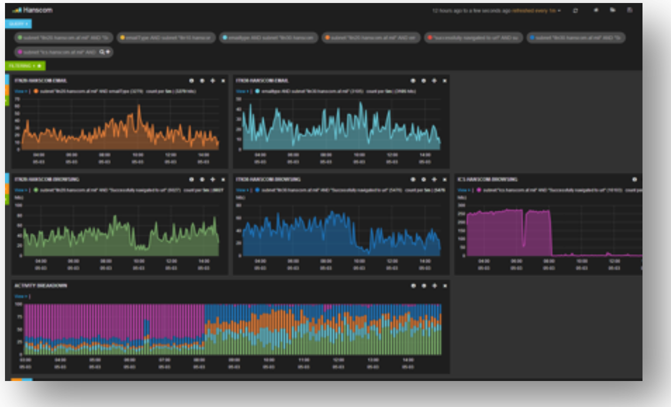
BREACH: Attack Platform, Reports
OPFOR: Opposing Force, Attacker
WORMHOLE: 0-day attack surrogates

Assessment Tools

Network Monitoring & MISSION REPLAY

Visualize traffic flows; replay attacker actions



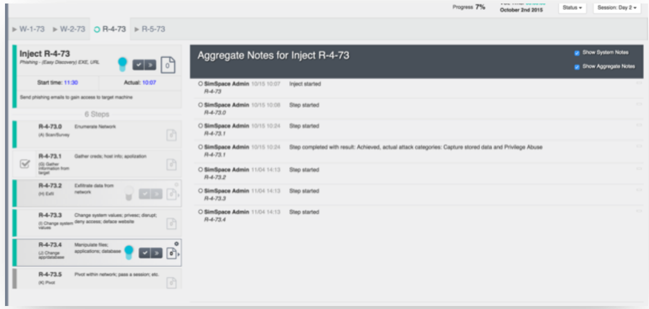


Traffic Generation STATUS

Monitor emulated user activity

Event TRACKING

Coordinate, record actions from Red & Blue



Progress 7%   October 2nd 2015   Status ▾   Session: Day 2 ▾

▶ W-1-73   ▶ W-2-73   ○ R-4-73   ▶ R-5-73

Inject R-4-73
Phishing - (Easy Discovery) EXE, URL

Start time: 11:30   Actual: 10:07

Send phishing emails to gain access to target machine

6 Steps

R-4-73.0 (A) Scan/Survey — Enumerate Network

☑ R-4-73.1 (G) Gather information from target — Gather creds; host info; apolization

R-4-73.2 (H) Exfil — Exfiltrate data from network

R-4-73.3 (I) Change system values — Change system values; privesc; disrupt; deny access; deface website

R-4-73.4 (J) Change app/database — Manipulate files; applications; database

R-4-73.5 (K) Pivot — Pivot within network; pass a session; etc.

Aggregate Notes for Inject R-4-73   ☑ Show System Notes   ☑ Show Aggregate Notes

○ **SimSpace Admin** 10/15 10:07 Inject started
R-4-73

○ **SimSpace Admin** 10/15 10:08 Step started
R-4-73.0

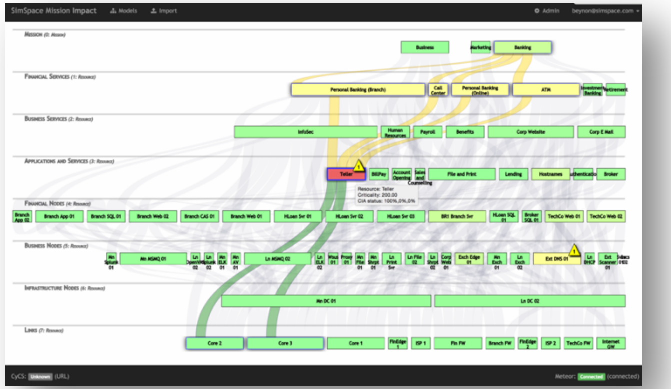
○ **SimSpace Admin** 10/15 10:24 Step started
R-4-73.1

○ **SimSpace Admin** 10/15 10:24 Step completed with result: Achieved, actual attack categories: Capture stored data and Privilege Abuse
R-4-73.1

○ **SimSpace Admin** 11/04 14:13 Step started
R-4-73.2

○ **SimSpace Admin** 11/04 14:13 Step started
R-4-73.3

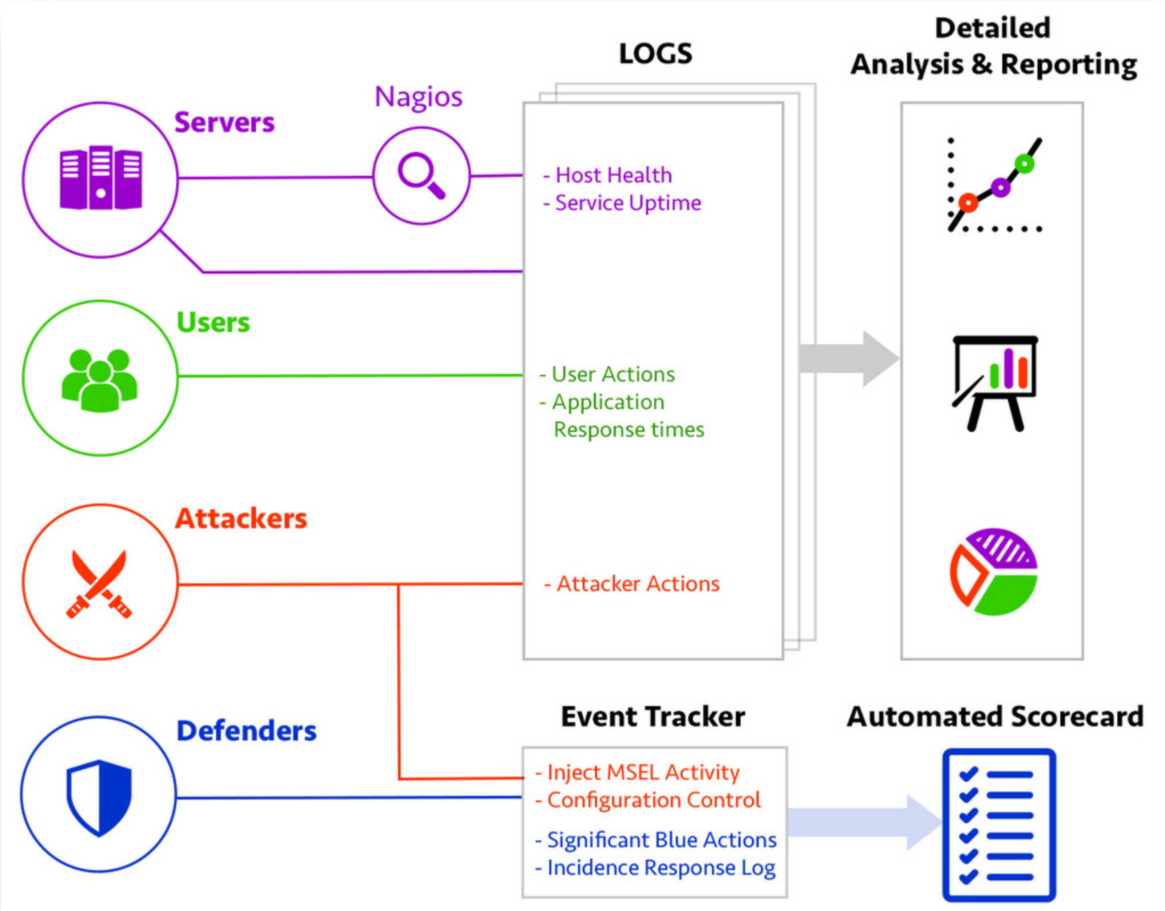
○ **SimSpace Admin** 11/04 14:13 Step started
R-4-73.4



Mission Impact DISPLAY

Business function dependencies on IT assets

Data Collection and Reporting



Data collected from multiple sources to provide reports, mission impact and scorecards

Detailed information collected from each emulated user about application and host performance

Example Uses

R&D

On-demand network environments and tools to develop novel cybersecurity solutions

TESTING

Assess products across suite of network environments and attack scenarios

ANALYSIS

Run the latest malware and attacks for analysis in a safe laboratory environment

ASSESSMENTS

Test your tools, people and processes against a suite of attack scenarios to identify areas for improvement

TRAINING

Team-based training against sophisticated adversaries in a safe and controlled environment

EXERCISES

Test your organizational preparedness to withstand sophisticated attacks and disruptive events

COMPLIANCE

For regulated industries leverage the network clone for compliance stress testing

SALES & POCs

Showcase product capabilities in a realistic and representative enterprise environment

SimSpace

Boston, MA (HQ)

51 Melcher St.
Boston, MA 02210
www.simspace.com

CONTACT US

William Hutchison, CEO
Hutch@simspace.com
Lee Rossey, CTO
Lee@simspace.com
Bart Gray, COO
Bartman@simspace.com

Sales & Business
sales@simspace.com
General Inquiry
contact@simspace.com
Tech Support
support@simspace.com

Example Products Used in the Range

- Any tool that can run in VMWare
- Operating Systems:
  - Windows servers & clients, Ubuntu, Kali
- Applications
  - MS Office, IE, Chrome, Firefox
  - Active Directory, Exchange, IIS, Apache, …
- Security Tools:
  - Symantec SEP, McAffee ePO
  - RSA Netwitness, Tanium, GRR
  - Splunk, Kibana, Snort, Bro, Alien Vault
  - CyberReason, Carbon Black - Bit9
  - Many others …

Example software that can be deployed

GoogleChrome
flashplayerplugin
git.install
notepadplusplus.install
javaruntime
7zip.install
adobereader
vlc
dotnet4.5
vcredist2010
winpcap
wamp-server
atom
nodejs.install
ccleaner
sysinternals
filezilla
vim
putty.install
libreoffice
mysql.workbench
paint.net
svn
hg
curl
pdfcreator
wget
calibre

wireshark
gimp
sourcetree
dotnet3.5
python2
cdburnerxp
baretail
foxitreader
firefox
0ad
microsoftsecurityessentials
audacity
defraggler
steam
speccy
tor-browser
1password
jdk7
nmap
pidgin
googleearth
emacs
cpu-z
innosetup
powergui
ffmpeg
eclipse

make
sudo
awscli
autoit
openoffice
logparser
directorymonitor
popcorntime
spybot
ie11
mobaxterm
openvpn
redis
autoruns
vmwareplayer
aimp
packer
cyberduck.install
intellijidea-community
bginfo
filezilla.server
bleachbit
xbmc
nscp
vmwarevsphereclient
hxd
sharex
btsync

cygwin
malwarebytes
nant
console2
chromium
windirstat
Tortoisesvn
blender
jenkins
nxlog
lastpass
combofix
ultravnc
r.Project
golang
openssl.light
poweriso
clamwin
pycharm-community
webstorm
logmein.client
httrack.app
Jrt
keepass.install
silverlight
rsat
sqlite