

# Black Hat Web Series BleedingBit and IOT devices



1 c04912106, March 2018, Rev. 11

#### **F**

### Future Workplace

Driven by changes in how people are working – and what they need from the office environment

#### Traditional office

#### Emerging office

More informal meeting areas for co-creation, collaboration



Work outside the traditional office increasing







Home

Cafe/public space

Airplane

Agile workspaces for individual productivity Interactive conference rooms for meetings, collaboration

Integrated communal spaces for socialization, play, wellness



### Today's Meeting Room Technology

The market is busy innovating, and technology options are multiplying

#### Simplified Projection

#### Team collaboration devices





### The Changing Threat Landscape

#### Commercialization of attack software

Blackhole	STATISTIC	S BLC	BLOCKED STATISCTICS		THREADS	FILES	SOFT VERSIONS	SECURITY	PREF	ERENCES		LOGOL
				or ANY proje	cts / content, Exp	perience 6	ame/javascript code. + years in the market. Th ER, LR, PM, WM. For malw					
Start date:	End d	late:		Thread:	All threads		Apply 5 se	ec[	]			
STATISTICS							05	HITED	HOSTS	LOADS	%•↓	Þ
TOTAL INFO					0 4 40	,	Indows 2000	36	14	1	7.14	
35114 (112) 19	0116 (HOSTS)	406 🚥	MOS		2.14%	-	💐 Windows XP	5338	3154	129	4.12	
					LOAD	s	a Windows 2003	70	35	1	2.86	
							💿 Windows Vista	3962	1982	47	2.40	
TODAY INFO 35114 (HTTD) 19	0116 (HOSTS)	406 🧰	ADS		2.14%		Windows 7	18763	9817	228	2.34	
•							THREADS	HITED	HOSTS	LOADS	%o ↓	je.
							zer0	35114	19116	406	2.14	
BROWSERS	HITED	HOSTS	LOADS	% ↓		۶ 						
💋 MSIE	23437	11664	333	2.88			EXPLOITS			LOADS	%o ↓	je.
😻 Firefox	2279	1585	38	2.42			🌾 PDF LIBTIFF			57	100.0(	
📀 Chrome	3340	2394	20	0.84 🥌			👾 Java Pack			349	1.85	
O Opera	1500	599	3	0.51								
							REFERERS	HITED	HOSTS	LOADS	•%o ↓	P
COUNTRIES	HITED	HOSTS	LOADS	%-↓		p.	sprevomations con	31620	17758	384	2.18	
🞾 Djibouti	3	2	1	50.00 🗲			proph.com	151	51	1	1.96	
Italy	7	3	1	33.33 💳			spatter can	20	4	0	0.00	
🥅 Germany	27	24	3	12.50 🗨			1000.000	17	2	0	0.00	
Other country	137	92	6	6.59 💶			lang.com	2	1	0	0.00	
🖭 Canada	41	34	1	3.03 💷			standary con	2	2	0	0.00	
🥮 United States	34809	18902	394	2.10			go com 4 Maggari A	1	1	0	0.00	
🖸 Pakistan	1	1	0	0.00 🥌			Rep. cm	43	12	0	0.00	
Philippines	1	1	0	0.00			particular com-	23	3	0	0.00	

Black-hole Exploit Service Command Console



#### Autosploit loader





### Context setting: Gartner IoT Reference Model







### Required Next Steps





### Print jobs on network









Payroll information: John Doe \$32,000



estination 92.168.0.51 92.168.0.51 92.168.0.109 92.168.0.51 92.168.0.51



#### Android July 2019 Security Update Patches 33 New Vulne

🛗 July 02, 2019 🛛 🛔 Swati Khandelwal

Secure

https://source.android.com/security/bulletin/2019-07-01

More .

#### Amazon Admits Alexa Voice Recordings Saved Indefinitely

#### Overview Advisories · Android Buileting · 2019 Builetins Jub June May April March February January Index > 2018 Bulleting > 2017 Bulleting > 2016 Bulleting > 2015 Bulletins Pixel/Nexus Bulletins

Source

https://thehackernews.com/2019/07/a update.html?utm\_source=feedburner8 +Cyber+Security+Blog%29&\_m=3n.00

# Print-related data breaches affected 60% of businesses last year

Q Se

By Anthony Spadafora February 12, 2019 Internet

Print is a growing security concern

🚯 💟 😰 🖸



nazon-admits-alexa-voice-reco



https://www.techradar.com/news/print-related-data-breaches-affected-60-of-businesses-last-year

### NSA Presentation at RSA 2018

- 93% of 2017 incidents preventable with best practices
- In 2018, NSA stated 90% of cyber incidents due to human error

# GOOD CYBER HYGIENE



### United Kingdom National Audit Office

#### • 80% of cyber attacks preventable with basic cyber hygiene

# **BASIC CYBER HYGIENE**



©2017 HP Inc. | All rights reserved. Content is subject to change without notice. | HP Confidential Key Takeaways

### 1. Every purchase decision is a SECURITY decision

- 2. CIO & CISO must get involved early in all endpoint procurement to ensure and drive security requirements into the endpoint procurement decisions
- 3. On-going assessment and monitoring of endpoint risks
- 4. Increase data controls for endpoint devices

- 5. Data breach monitoring and reporting for all endpoints
- 6. On-going evaluation and monitoring of endpoint protections deployed
- 7. Treat endpoint devices as the first line of defense
- 8. Include all endpoint devices in your policies and security action plans





# Thank you

# Ronald.Chestang@hp.com



<u>www.hp.com/thewolf</u> <u>www.hp.com/reinventsecurity</u>

Copyright 2018 HP Development Company, L.P. The information contained herein is subject to change without notice.