1. Tổng quan

Credential Dumping là kỹ thuật mà kẻ tấn công sử dụng để trích xuất thông tin chứng thực (mật khẩu, hash, token) từ hệ thống bị xâm. Các nguồn dữ liệu điển hình bao gồm SAM, NTDS, /etc/shadow, hoặc trực tiếp từ bộ nhớ (process memory). Kỹ thuật này thường nhằm mục tiêu mở rộng truy cập trong mạng nội bộ và hỗ trợ lateral movement.

Mục tiêu báo cáo: mô tả kỹ thuật, các biến thể, phương pháp phát hiện, mitigation, và cung cấp một bảng sự kiện mẫu lớn phục vụ cho bài lab / phân tích forensics.

2. Chi tiết kỹ thuật

Các phương thức credential dumping phổ biến:

- Đọc trực tiếp tệp lưu trữ chứng thực: ví dụ /etc/shadow trên Linux, SAM/NTDS trên Windows.
- Dump từ bộ nhớ: đọc process memory của tiến trình lưu giữ thông tin chứng thực (ví dụ LSASS trên Windows).
- Sử dụng công cụ/tiện ích: mimikatz, gsecdump, pwdump, creddump, secretos.
- Lấy thông tin từ file cấu hình, script hoặc backup không được mã hóa.

Lưu ý về môi trường: hệ thống Windows thường lưu nhiều thông tin nhạy cảm trong memory của tiến trình LSASS hoặc trong AD database (NTDS.dit). Trên Linux, file /etc/shadow và các file cấu hình ứng dụng là mục tiêu.

3. Kịch bản tấn công

Mô tả kịch bản: Kẻ tấn công xâm nhập một host công cộng (ví dụ quản trị từ xa), cài payload để thu thập hash từ LSASS, crack hoặc reuse hash để SSH sang host khác, từ đó truy cập database chứa dữ liệu nhạy cảm.

Chi tiết bước:

1) Recon - tìm host quản trị và các tài khoản có quyền cao.
2) Initial Access - khai thác vuln hoặc sử dụng credential phishing để có foothold.
3) Dump - sử dụng công cụ để dump memory/credential stores.
4) Abuse - sử dụng credential để di chuyển ngang hoặc nâng quyền.
5) Persistence & Exfil - cài backdoor và exfil dữ liệu.

4. Phát hiện và biện pháp giảm thiểu

Phát hiện:

- Giám sát hoạt động tiến trình bất thường (lsass.exe memory read, procdump usage).
- Tìm kiếm hành vi dump file, outbound connections sau khi dump.
- Sử dụng YARA/Suricata để phát hiện chuỗi đặc trưng.

Giảm thiểu:

- Bật LAPS / Credential Guard trên Windows, áp dụng EDR.
- Hạn chế quyền: least privilege, segment network.
- Bảo vệ tệp nhạy cảm (chặn truy cập /etc/shadow), áp dụng mật khẩu mạnh và 2FA.

5. Hướng dẫn triển khai Lab

Phần này mô tả cách sử dụng bảng sự kiện mẫu trong quá trình lab: cách dựng môi trường, tạo activity mô phỏng, và cách dùng bảng sự kiện để thực hành phân tích.

Mẹo: Sử dụng docker-compose để dựng mạng lab, seed file logs và script simulate_swipe.sh / simulate_lsass_dump.sh để tạo các sự kiện tương ứng.

Bảng sự kiện chi tiết (dùng cho phân tích forensic)

Bảng dưới đây liệt kê nhiều sự kiện liên quan đến credential dumping và hoạt động tấn công liên quan. Bảng có nhiều hàng để đảm bảo trải dài qua nhiều trang, thuận tiện cho bài tập phân tích log.

Bảng dữ liệu credential dump

Timestamp	Host	Event	Source IP	File/Hash	Action
2013-11-29 00:00:00	ADMIN-01	LSASS Dump Detected	10.0.7.190	lsass.dmp / SHA256: b9c402da05821277	Possible credential exfil from memory
2013-11-29 00:05:00	STAGE-01	Suspicious Process Spawn	10.0.8.122	proc: unknown_exec / SHA256: 1f82ddeb7dc7c714	Spawned by user 'svc_hvac'
2013-11-29 00:10:00	STAGE-01	Service Installed	10.0.7.96	service: backdoor_svc	Service started at boot
2013-11-29 00:15:00	WEB-01	Config File Read	10.0.10.42	config.ini	Credentials found in config
2013-11-29 00:20:00	POS-01	SSH Login	10.0.1.219	n/a	Login successful (possible credential reuse)
2013-11-29 00:25:00	DB-01	LSASS Dump Detected	10.0.3.106	lsass.dmp / SHA256: d19684345abce819	Possible credential exfil from memory
2013-11-29 00:30:00	POS-02	Process Memory Read	10.0.10.12	blackpos-lab.bin / SHA256: 99129601fa0661f2	Credential pattern found
2013-11-29 00:35:00	WORKSTATION-12	SSH Login	10.0.8.60	n/a	Login successful (possible credential reuse)

2013-11-29 00:40:00	POS-01	Service Installed	10.0.9.119	service: backdoor_svc	Service started at boot
2013-11-29 00:45:00	POS-02	FTP Upload Attempt	10.0.9.114	cards-20131129_part5.csv / SHA256: d0fef2e4262d8d25	Outbound to ftp-exfil-targetlab.example
2013-11-29 00:50:00	WORKSTATION-12	Scheduled Task Creation	10.0.5.205	task: persist_worker	Persistence scheduled
2013-11-29 00:55:00	WEB-01	SSH Login	10.0.7.58	n/a	Login successful (possible credential reuse)
2013-11-29 01:00:00	ADMIN-01	SQL Dump	10.0.2.96	db-dump-20131129.sql / SHA256: e84fbab96c874f7f	Sensitive data exported
2013-11-29 01:05:00		Config File Read			Credentials found in config
2013-11-29 01:10:00	WEB-01	Process Memory Read	10.0.2.228	blackpos-lab.bin / SHA256: 29bd38d37a50e15b	Credential pattern found
2013-11-29 01:15:00	ADMIN-01	Config File Read	10.0.9.223	config.ini	Credentials found in config
2013-11-29 01:20:00	VPN-01	SSH Login	10.0.10.140	n/a	Login successful (possible credential reuse)
2013-11-29 01:25:00	PROXY-01	SQL Dump	10.0.10.80	db-dump-20131129.sql / SHA256: 0a377e6ab46b1848	Sensitive data exported
2013-11-29 01:30:00	LSASS-BOX	FTP Upload Attempt	10.0.9.93	cards-20131129_part3.csv / SHA256: 9655ff022efeeab0	Outbound to ftp-exfil-targetlab.example

2013-11-29 01:35:00	PROXY-01	SSH Login	10.0.8.13	n/a	Login successful (possible credential reuse)
2013-11-29 01:40:00	STAGE-01	Scheduled Task Creation	10.0.4.118	task: persist_worker	Persistence scheduled
2013-11-29 01:45:00	WORKSTATION-12	Config File Read	10.0.8.188	config.ini	Credentials found in config
2013-11-29 01:50:00	ADMIN-01	Config File Read	10.0.6.134	config.ini	Credentials found in config
2013-11-29 01:55:00	POS-01	Scheduled Task Creation	10.0.7.53	task: persist_worker	Persistence scheduled
2013-11-29 02:00:00	LSASS-BOX	Scheduled Task Creation	10.0.8.36	task: persist_worker	Persistence scheduled
2013-11-29 02:05:00	VPN-01	LSASS Dump Detected	10.0.4.220	lsass.dmp / SHA256: 8bd952f21211d778	Possible credential exfil from memory
2013-11-29 02:10:00	LSASS-BOX	Scheduled Task Creation	10.0.8.104	task: persist_worker	Persistence scheduled
2013-11-29 02:15:00	STAGE-01	FTP Upload Attempt	10.0.4.188	cards-20131129_part5.csv / SHA256: beddff63db8a35f1	Outbound to ftp-exfil-targetlab.example
2013-11-29 02:20:00	ADMIN-01	Config File Read	10.0.8.142	config.ini	Credentials found in config
2013-11-29 02:25:00	DB-01	SQL Dump	10.0.9.234	db-dump-20131129.sql / SHA256: 1949c9ffcd5ea198	Sensitive data exported
2013-11-29 02:30:00	WORKSTATION-12	LSASS Dump Detected	10.0.8.150	lsass.dmp / SHA256: 31acd7e7fbd13b07	Possible credential exfil from memory

2013-11-29 02:35:00	DB-01	Large POST to external	10.0.6.134	cards-20131129_part8.csv / SHA256: 1acef8425062d864	Outbound to ftp-exfil-targetlab.example
2013-11-29 02:40:00	WORKSTATION-12	FTP Upload Attempt	10.0.5.113	cards-20131129_part2.csv / SHA256: 3f95ad26ab122140	Outbound to ftp-exfil-targetlab.example
2013-11-29 02:45:00	WEB-01	SSH Login	10.0.2.60	n/a	Login successful (possible credential reuse)
2013-11-29 02:50:00	WEB-01	SSH Login	10.0.6.170	n/a	Login successful (possible credential reuse)
2013-11-29 02:55:00	ADMIN-01	Config File Read	10.0.5.171	config.ini	Credentials found in config
2013-11-29 03:00:00	POS-01	Scheduled Task Creation	10.0.7.195	task: persist_worker	Persistence scheduled
2013-11-29 03:05:00	POS-01	FTP Upload Attempt	10.0.4.41	cards-20131129_part8.csv / SHA256: 7d992b1dcda137f9	Outbound to ftp-exfil-targetlab.example
2013-11-29 03:10:00	PROXY-01	LSASS Dump Detected	10.0.7.207	lsass.dmp / SHA256: fbcecbaf2dd1066f	Possible credential exfil from memory
2013-11-29 03:15:00	WORKSTATION-12	Large POST to external	10.0.4.14	cards-20131129_part6.csv / SHA256: 2bdcb8927f505792	Outbound to ftp-exfil-targetlab.example
2013-11-29 03:20:00	VPN-01	SQL Dump	10.0.5.181	db-dump-20131129.sql / SHA256:	Sensitive data exported

				b26468dfed17825f	
2013-11-29 03:25:00	LSASS-BOX	SQL Dump	10.0.10.177	db-dump-20131129.sql / SHA256: 70e075d63ddda7ac	Sensitive data exported
2013-11-29 03:30:00	VPN-01	Process Memory Read	10.0.2.74	blackpos-lab.bin / SHA256: 8d6f97856397c9f1	Credential pattern found
2013-11-29 03:35:00	ADMIN-01	LSASS Dump Detected	10.0.2.222	lsass.dmp / SHA256: 43607084bb5a3223	Possible credential exfil from memory
2013-11-29 03:40:00	STAGE-01	LSASS Dump Detected	10.0.7.163	lsass.dmp / SHA256: 8d6b20250bad1d86	Possible credential exfil from memory
2013-11-29 03:45:00	STAGE-01	SSH Login	10.0.6.52	n/a	Login successful (possible credential reuse)
2013-11-29 03:50:00	STAGE-01	Scheduled Task Creation	10.0.7.252	task: persist_worker	Persistence scheduled
2013-11-29 03:55:00	DB-01	FTP Upload Attempt	10.0.7.173	cards-20131129_part5.csv / SHA256: 1d08a515d606cefa	Outbound to ftp-exfil-targetlab.example
2013-11-29 04:00:00	VPN-01	Scheduled Task Creation	10.0.2.238	task: persist_worker	Persistence scheduled
2013-11-29 04:05:00	PROXY-01	LSASS Dump Detected	10.0.9.67	lsass.dmp / SHA256: 387249bd316e85a7	Possible credential exfil from memory
2013-11-29 04:10:00	STAGE-01	Large POST to external	10.0.5.180	cards-20131129_part2.csv / SHA256: 846147560642fc8a	Outbound to ftp-exfil-targetlab.example

2013-11-29 04:15:00	LSASS-BOX	FTP Upload Attempt	10.0.1.77	cards-20131129_part4.csv / SHA256: 2146c12be4da2470	Outbound to ftp-exfil-targetlab.example
2013-11-29 04:20:00	POS-02	LSASS Dump Detected	10.0.1.192	lsass.dmp / SHA256: a3a847cbfb46feec	Possible credential exfil from memory
2013-11-29 04:25:00	POS-01	Suspicious Process Spawn	10.0.4.4	proc: unknown_exec / SHA256: ca09f69ea5c9933e	Spawned by user 'svc_hvac'
2013-11-29 04:30:00	STAGE-01	FTP Upload Attempt	10.0.6.112	cards-20131129_part10.csv / SHA256: b026418045dc86e3	Outbound to ftp-exfil-targetlab.example
2013-11-29 04:35:00	VPN-01	LSASS Dump Detected	10.0.7.125	lsass.dmp / SHA256: 573e245a5953a2c1	Possible credential exfil from memory
2013-11-29 04:40:00	DB-01	SSH Login	10.0.5.13	n/a	Login successful (possible credential reuse)
2013-11-29 04:45:00	STAGE-01	Large POST to external	10.0.5.53	cards-20131129_part2.csv / SHA256: 990afed33020d1a8	Outbound to ftp-exfil-targetlab.example
2013-11-29 04:50:00	PROXY-01	Service Installed	10.0.3.209	service: backdoor_svc	Service started at boot
2013-11-29 04:55:00	POS-01	Large POST to external	10.0.8.123	cards-20131129_part7.csv / SHA256: 8235dca3a59763b6	Outbound to ftp-exfil-targetlab.example
2013-11-29 05:00:00	DB-01	Process Memory Read	10.0.2.129	blackpos-lab.bin / SHA256:	Credential pattern found

				3b6263199a08826e	
2013-11-29 05:05:00	VPN-01	Suspicious Process Spawn	10.0.5.239	proc: unknown_exec / SHA256: 27eed54ace18372e	Spawned by user 'svc_hvac'
2013-11-29 05:10:00	POS-02	SSH Login	10.0.6.158	n/a	Login successful (possible credential reuse)
2013-11-29 05:15:00	LSASS-BOX	SSH Login	10.0.10.147	n/a	Login successful (possible credential reuse)
2013-11-29 05:20:00	DB-01	Process Memory Read	10.0.1.148	blackpos-lab.bin / SHA256: 96f82f754c9129fa	Credential pattern found
2013-11-29 05:25:00	POS-01	Suspicious Process Spawn	10.0.9.180	proc: unknown_exec / SHA256: c91dc4d99869a506	Spawned by user 'svc_hvac'
2013-11-29 05:30:00	LSASS-BOX	Service Installed	10.0.1.153	service: backdoor_svc	Service started at boot
2013-11-29 05:35:00	LSASS-BOX	FTP Upload Attempt	10.0.6.17	cards-20131129_part7.csv / SHA256: 1d4ed652ec76f995	Outbound to ftp-exfil-targetlab.example
2013-11-29 05:40:00	LSASS-BOX	FTP Upload Attempt	10.0.2.180	cards-20131129_part6.csv / SHA256: 91b946a3f54dc62e	Outbound to ftp-exfil-targetlab.example
2013-11-29 05:45:00	POS-02	Suspicious Process Spawn	10.0.5.146	proc: unknown_exec / SHA256: 373b6d8d4b25f9cd	Spawned by user 'svc_hvac'

2013-11-29 05:50:00	PROXY-01	Process Memory Read	10.0.3.39	blackpos-lab.bin / SHA256: 58f28fcd4ee3bc09	Credential pattern found
2013-11-29 05:55:00	PROXY-01	SSH Login	10.0.3.47	n/a	Login successful (possible credential reuse)
2013-11-29 06:00:00	WEB-01	LSASS Dump Detected	10.0.2.235	lsass.dmp / SHA256: 667671af8708a70f	Possible credential exfil from memory
2013-11-29 06:05:00	VPN-01	FTP Upload Attempt	10.0.10.6	cards-20131129_part4.csv / SHA256: 6591105b19efe558	Outbound to ftp-exfil-targetlab.example
2013-11-29 06:10:00	WORKSTATION-12	Config File Read	10.0.7.212	config.ini	Credentials found in config
2013-11-29 06:15:00	VPN-01	FTP Upload Attempt	10.0.4.90	cards-20131129_part7.csv / SHA256: 585f7d0ff19289d5	Outbound to ftp-exfil-targetlab.example
2013-11-29 06:20:00	DB-01	Config File Read	10.0.9.131	config.ini	Credentials found in config
2013-11-29 06:25:00	DB-01	Large POST to external	10.0.6.209	cards-20131129_part4.csv / SHA256: 12b770e02fcfde95	Outbound to ftp-exfil-targetlab.example
2013-11-29 06:30:00	POS-01	FTP Upload Attempt	10.0.5.156	cards-20131129_part7.csv / SHA256: 45ddcac5ba881906	Outbound to ftp-exfil-targetlab.example
2013-11-29 06:35:00	WORKSTATION-12	Large POST to external	10.0.6.76	cards-20131129_part9.csv / SHA256: d1eabd81c82a9bd0	Outbound to ftp-exfil-targetlab.example

2013-11-29 06:40:00	LSASS-BOX	Suspicious Process Spawn	10.0.5.163	proc: unknown_exec / SHA256: 25ebe27973dec46f	Spawned by user 'svc_hvac'
2013-11-29 06:45:00	VPN-01	Large POST to external	10.0.9.2	cards-20131129_part8.csv / SHA256: 4c4eec07c64c6b94	Outbound to ftp-exfil-targetlab.example
2013-11-29 06:50:00	DB-01	Large POST to external	10.0.2.135	cards-20131129_part5.csv / SHA256: cfe73d1ffe063ee5	Outbound to ftp-exfil-targetlab.example
2013-11-29 06:55:00	LSASS-BOX	SQL Dump	10.0.10.199	db-dump-20131129.sql / SHA256: 2744b59f8584afeb	Sensitive data exported
2013-11-29 07:00:00	POS-02	Suspicious Process Spawn	10.0.8.112	proc: unknown_exec / SHA256: c7ad6e872c0a4c9b	Spawned by user 'svc_hvac'
2013-11-29 07:05:00	WEB-01	Large POST to external	10.0.10.94	cards-20131129_part9.csv / SHA256: 7d9314a396f20570	Outbound to ftp-exfil-targetlab.example
2013-11-29 07:10:00	STAGE-01	Service Installed	10.0.6.90	service: backdoor_svc	Service started at boot
2013-11-29 07:15:00	ADMIN-01	Scheduled Task Creation	10.0.10.243	task: persist_worker	Persistence scheduled
2013-11-29 07:20:00	STAGE-01	LSASS Dump Detected	10.0.8.12	lsass.dmp / SHA256: 84193ae1a6dcfbcd	Possible credential exfil from memory
2013-11-29 07:25:00	POS-01	Service Installed	10.0.9.56	service: backdoor_svc	Service started at boot

2013-11-29 07:30:00	DB-01	SSH Login	10.0.8.207	n/a	Login successful (possible credential reuse)
2013-11-29 07:35:00	LSASS-BOX	Config File Read	10.0.3.86	config.ini	Credentials found in config
2013-11-29 07:40:00	DB-01	SSH Login	10.0.6.19	n/a	Login successful (possible credential reuse)
2013-11-29 07:45:00	POS-01	SQL Dump	10.0.5.239	db-dump-20131129.sql / SHA256: a8b8817bf3d761f7	Sensitive data exported
2013-11-29 07:50:00	ADMIN-01	Service Installed	10.0.2.50	service: backdoor_svc	Service started at boot
2013-11-29 07:55:00	WORKSTATION-12	Suspicious Process Spawn	10.0.2.83	proc: unknown_exec / SHA256: 51402279fa6e9e2a	Spawned by user 'svc_hvac'
2013-11-29 08:00:00	STAGE-01	Scheduled Task Creation	10.0.9.127	task: persist_worker	Persistence scheduled
2013-11-29 08:05:00	WORKSTATION-12	FTP Upload Attempt	10.0.5.146	cards-20131129_part8.csv / SHA256: 58364e3a8790adc5	Outbound to ftp-exfil-targetlab.example
2013-11-29 08:10:00	POS-02	SQL Dump	10.0.6.219	db-dump-20131129.sql / SHA256: 950481b02b5e06f3	Sensitive data exported
2013-11-29 08:15:00	POS-01	FTP Upload Attempt	10.0.4.213	cards-20131129_part3.csv / SHA256: 597ba5041e013ab6	Outbound to ftp-exfil-targetlab.example

2013-11-29 08:20:00	DB-01	LSASS Dump Detected	10.0.7.148	lsass.dmp / SHA256: d7154c4a60625256	Possible credential exfil from memory
2013-11-29 08:25:00	STAGE-01	Large POST to external	10.0.4.141	cards-20131129_part2.csv / SHA256: 10003b7a20751ea1	Outbound to ftp-exfil-targetlab.example
2013-11-29 08:30:00	STAGE-01	Scheduled Task Creation	10.0.10.198	task: persist_worker	Persistence scheduled
2013-11-29 08:35:00	DB-01	SQL Dump	10.0.2.107	db-dump-20131129.sql / SHA256: 6818c26f1fbd7ed7	Sensitive data exported
2013-11-29 08:40:00	VPN-01	FTP Upload Attempt	10.0.5.135	cards-20131129_part1.csv / SHA256: 966b0e15f7e1ca14	Outbound to ftp-exfil-targetlab.example
2013-11-29 08:45:00	VPN-01	Process Memory Read	10.0.8.103	blackpos-lab.bin / SHA256: 3d7430fe33854c22	Credential pattern found
2013-11-29 08:50:00	STAGE-01	FTP Upload Attempt	10.0.1.136	cards-20131129_part4.csv / SHA256: 908deb054564c783	Outbound to ftp-exfil-targetlab.example
2013-11-29 08:55:00	PROXY-01	SQL Dump	10.0.2.17	db-dump-20131129.sql / SHA256: c7b145ea7431a2d5	Sensitive data exported
2013-11-29 09:00:00	LSASS-BOX	Large POST to external	10.0.3.221	cards-20131129_part7.csv / SHA256: 7500829e888145d0	Outbound to ftp-exfil-targetlab.example
2013-11-29 09:05:00	ADMIN-01	SSH Login	10.0.7.233	n/a	Login successful (possible

					credential reuse)
2013-11-29 09:10:00	STAGE-01	Service Installed	10.0.10.107	service: backdoor_svc	Service started at boot
2013-11-29 09:15:00	STAGE-01	Service Installed	10.0.9.249	service: backdoor_svc	Service started at boot
2013-11-29 09:20:00	WORKSTATION-12	Service Installed	10.0.4.19	service: backdoor_svc	Service started at boot
2013-11-29 09:25:00	LSASS-BOX	FTP Upload Attempt	10.0.4.7	cards-20131129_part6.csv / SHA256: 45b0cda00ff43595	Outbound to ftp-exfil-targetlab.example
2013-11-29 09:30:00	STAGE-01	Scheduled Task Creation	10.0.7.31	task: persist_worker	Persistence scheduled
2013-11-29 09:35:00	ADMIN-01	Service Installed	10.0.8.20	service: backdoor_svc	Service started at boot
2013-11-29 09:40:00	POS-01	Suspicious Process Spawn	10.0.8.162	proc: unknown_exec / SHA256: dc79ec9313294407	Spawned by user 'svc_hvac'
2013-11-29 09:45:00	PROXY-01	FTP Upload Attempt	10.0.1.122	cards-20131129_part10.csv / SHA256: 15262acad16be89d	Outbound to ftp-exfil-targetlab.example
2013-11-29 09:50:00	WORKSTATION-12	SQL Dump	10.0.9.203	db-dump-20131129.sql / SHA256: ca3aaf4cde2695d7	Sensitive data exported
2013-11-29 09:55:00	STAGE-01	Config File Read	10.0.10.79	config.ini	Credentials found in config
2013-11-29 10:00:00	WEB-01	Suspicious Process Spawn	10.0.1.174	proc: unknown_exec / SHA256:	Spawned by user 'svc_hvac'

				2a5243398731c6d6	
2013-11-29 10:05:00	ADMIN-01	Config File Read	10.0.1.81	config.ini	Credentials found in config
2013-11-29 10:10:00	STAGE-01	SQL Dump	10.0.3.72	db-dump-20131129.sql / SHA256: 84acea8d005cb2c4	Sensitive data exported
2013-11-29 10:15:00	VPN-01	FTP Upload Attempt	10.0.10.207	cards-20131129_part2.csv / SHA256: e9532cd3e5928eae	Outbound to ftp-exfil-targetlab.example
2013-11-29 10:20:00	WEB-01	Scheduled Task Creation	10.0.2.189	task: persist_worker	Persistence scheduled
2013-11-29 10:25:00	PROXY-01	Config File Read	10.0.5.71	config.ini	Credentials found in config
2013-11-29 10:30:00	STAGE-01	SSH Login	10.0.5.88	n/a	Login successful (possible credential reuse)
2013-11-29 10:35:00	VPN-01	LSASS Dump Detected	10.0.10.5	lsass.dmp / SHA256: b0290303a758bb13	Possible credential exfil from memory
2013-11-29 10:40:00	WEB-01	SSH Login	10.0.7.237	n/a	Login successful (possible credential reuse)
2013-11-29 10:45:00	DB-01	Scheduled Task Creation	10.0.3.146	task: persist_worker	Persistence scheduled
2013-11-29 10:50:00	PROXY-01	Service Installed	10.0.8.239	service: backdoor_svc	Service started at boot
2013-11-29 10:55:00	WEB-01	Scheduled Task Creation	10.0.5.146	task: persist_worker	Persistence scheduled

2013-11-29 11:00:00	VPN-01	Scheduled Task Creation	10.0.3.128	task: persist_worker	Persistence scheduled
2013-11-29 11:05:00	DB-01	Suspicious Process Spawn	10.0.4.201	proc: unknown_exec / SHA256: 106068704ee01ddf	Spawned by user 'svc_hvac'
2013-11-29 11:10:00	WEB-01	Suspicious Process Spawn	10.0.2.240	proc: unknown_exec / SHA256: 7a64edd274697a16	Spawned by user 'svc_hvac'
2013-11-29 11:15:00	DB-01	Process Memory Read	10.0.7.68	blackpos-lab.bin / SHA256: e2bbaa394a53f999	Credential pattern found
2013-11-29 11:20:00	WEB-01	Scheduled Task Creation	10.0.3.160	task: persist_worker	Persistence scheduled
2013-11-29 11:25:00	WEB-01	Config File Read	10.0.6.208	config.ini	Credentials found in config
2013-11-29 11:30:00	POS-02	LSASS Dump Detected	10.0.8.130	lsass.dmp / SHA256: 6028a6f0e67a98d7	Possible credential exfil from memory
2013-11-29 11:35:00	DB-01	Config File Read	10.0.10.19	config.ini	Credentials found in config
2013-11-29 11:40:00	POS-02	Scheduled Task Creation	10.0.9.116	task: persist_worker	Persistence scheduled
2013-11-29 11:45:00	VPN-01	LSASS Dump Detected	10.0.3.198	lsass.dmp / SHA256: b2c011a3fb316592	Possible credential exfil from memory
2013-11-29 11:50:00	ADMIN-01	Large POST to external	10.0.4.229	cards-20131129_part5.csv / SHA256: 57502ba5380a9320	Outbound to ftp-exfil-targetlab.example

2013-11-29 11:55:00	STAGE-01	LSASS Dump Detected	10.0.8.202	lsass.dmp / SHA256: c9bc765f12bf3e4c	Possible credential exfil from memory
2013-11-29 12:00:00	WORKSTATION-12	Scheduled Task Creation	10.0.3.36	task: persist_worker	Persistence scheduled
2013-11-29 12:05:00	VPN-01	Scheduled Task Creation	10.0.3.160	task: persist_worker	Persistence scheduled
2013-11-29 12:10:00	POS-02	Scheduled Task Creation	10.0.5.201	task: persist_worker	Persistence scheduled
2013-11-29 12:15:00	STAGE-01	Process Memory Read	10.0.10.3	blackpos-lab.bin / SHA256: b6c8cdc8def6cbc8	Credential pattern found
2013-11-29 12:20:00	ADMIN-01	Config File Read	10.0.4.115	config.ini	Credentials found in config
2013-11-29 12:25:00	POS-02	Service Installed	10.0.6.89	service: backdoor_svc	Service started at boot
2013-11-29 12:30:00	POS-01	SQL Dump	10.0.5.229	db-dump-20131129.sql / SHA256: 84e1da2ce2801e21	Sensitive data exported
2013-11-29 12:35:00	DB-01	SSH Login	10.0.10.38	n/a	Login successful (possible credential reuse)
2013-11-29 12:40:00	WEB-01	Large POST to external	10.0.6.43	cards-20131129_part8.csv / SHA256: 4fe7dd1b54e63941	Outbound to ftp-exfil-targetlab.example
2013-11-29 12:45:00	POS-02	Config File Read	10.0.8.1	config.ini	Credentials found in config
2013-11-29 12:50:00	POS-01	Config File Read	10.0.2.134	config.ini	Credentials found in config

2013-11-29 12:55:00	PROXY-01	Suspicious Process Spawn	10.0.10.173	proc: unknown_exec / SHA256: 26001ad2132cc667	Spawned by user 'svc_hvac'
2013-11-29 13:00:00	WEB-01	LSASS Dump Detected	10.0.7.219	lsass.dmp / SHA256: 8ec4b6adfd72ecd9	Possible credential exfil from memory
2013-11-29 13:05:00	VPN-01	Scheduled Task Creation	10.0.8.71	task: persist_worker	Persistence scheduled
2013-11-29 13:10:00	ADMIN-01	SQL Dump	10.0.3.155	db-dump-20131129.sql / SHA256: c4dcbc4456165b7c	Sensitive data exported
2013-11-29 13:15:00	ADMIN-01	Process Memory Read	10.0.8.79	blackpos-lab.bin / SHA256: 529c19335be45215	Credential pattern found
2013-11-29 13:20:00	DB-01	Config File Read	10.0.3.106	config.ini	Credentials found in config
2013-11-29 13:25:00	PROXY-01	Scheduled Task Creation	10.0.1.149	task: persist_worker	Persistence scheduled
2013-11-29 13:30:00	WEB-01	Scheduled Task Creation	10.0.1.64	task: persist_worker	Persistence scheduled
2013-11-29 13:35:00	POS-01	Scheduled Task Creation	10.0.3.248	task: persist_worker	Persistence scheduled
2013-11-29 13:40:00	STAGE-01	Scheduled Task Creation	10.0.4.167	task: persist_worker	Persistence scheduled
2013-11-29 13:45:00	PROXY-01	Scheduled Task Creation	10.0.4.245	task: persist_worker	Persistence scheduled
2013-11-29 13:50:00	POS-01	Suspicious Process Spawn	10.0.10.145	proc: unknown_exec / SHA256: 26219d625a3e2750	Spawned by user 'svc_hvac'

2013-11-29 13:55:00	STAGE-01	SQL Dump	10.0.3.210	db-dump-20131129.sql / SHA256: 453b1ebbce374666	Sensitive data exported
2013-11-29 14:00:00	LSASS-BOX	Service Installed	10.0.6.241	service: backdoor_svc	Service started at boot
2013-11-29 14:05:00	DB-01	SQL Dump	10.0.1.99	db-dump-20131129.sql / SHA256: 826caffdc1af946b	Sensitive data exported
2013-11-29 14:10:00	PROXY-01	Scheduled Task Creation	10.0.3.68	task: persist_worker	Persistence scheduled
2013-11-29 14:15:00	WORKSTATION-12	SQL Dump	10.0.4.204	db-dump-20131129.sql / SHA256: c64dfe06934c4dde	Sensitive data exported
2013-11-29 14:20:00	STAGE-01	Process Memory Read	10.0.10.198	blackpos-lab.bin / SHA256: 35444b0e72b7569e	Credential pattern found
2013-11-29 14:25:00	WEB-01	Process Memory Read	10.0.3.166	blackpos-lab.bin / SHA256: c163460646b55e90	Credential pattern found
2013-11-29 14:30:00	POS-02	Scheduled Task Creation	10.0.1.199	task: persist_worker	Persistence scheduled
2013-11-29 14:35:00	POS-02	Large POST to external	10.0.1.251	cards-20131129_part4.csv / SHA256: 702046f0a5860505	Outbound to ftp-exfil-targetlab.example
2013-11-29 14:40:00	WEB-01	SSH Login	10.0.2.135	n/a	Login successful (possible credential reuse)

2013-11-29 14:45:00	VPN-01	Large POST to external	10.0.7.136	cards-20131129_part10.csv / SHA256: e95768a19f1ceef0	Outbound to ftp-exfil-targetlab.example
2013-11-29 14:50:00	ADMIN-01	Suspicious Process Spawn	10.0.9.101	proc: unknown_exec / SHA256: 6130b47147e15ec2	Spawned by user 'svc_hvac'
2013-11-29 14:55:00	WORKSTATION-12	SQL Dump	10.0.7.133	db-dump-20131129.sql / SHA256: 526252effea0ab56	Sensitive data exported
2013-11-29 15:00:00	DB-01	SQL Dump	10.0.8.70	db-dump-20131129.sql / SHA256: b8283af3567af33b	Sensitive data exported
2013-11-29 15:05:00	POS-01	LSASS Dump Detected	10.0.3.72	lsass.dmp / SHA256: f8e1a86a0450ace2	Possible credential exfil from memory
2013-11-29 15:10:00	POS-01	SSH Login	10.0.4.252	n/a	Login successful (possible credential reuse)
2013-11-29 15:15:00	VPN-01	Service Installed	10.0.4.196	service: backdoor_svc	Service started at boot
2013-11-29 15:20:00	POS-01	Suspicious Process Spawn	10.0.3.239	proc: unknown_exec / SHA256: 4b7e9d4b497ab147	Spawned by user 'svc_hvac'
2013-11-29 15:25:00	POS-02	Suspicious Process Spawn	10.0.4.213	proc: unknown_exec / SHA256: 0451dd1f5ffb6706	Spawned by user 'svc_hvac'

2013-11-29 15:30:00	WEB-01	FTP Upload Attempt	10.0.2.18	cards-20131129_part9.csv / SHA256: 11788df4eecba9ad	Outbound to ftp-exfil-targetlab.example
2013-11-29 15:35:00	PROXY-01	Suspicious Process Spawn	10.0.8.76	proc: unknown_exec / SHA256: 869c918ff18a36a9	Spawned by user 'svc_hvac'
2013-11-29 15:40:00	STAGE-01	Config File Read	10.0.2.89	config.ini	Credentials found in config
2013-11-29 15:45:00	STAGE-01	Large POST to external	10.0.10.224	cards-20131129_part8.csv / SHA256: 17faa7a766be7382	Outbound to ftp-exfil-targetlab.example
2013-11-29 15:50:00	POS-01	FTP Upload Attempt	10.0.3.167	cards-20131129_part6.csv / SHA256: ef9167aa8bd0d1fc	Outbound to ftp-exfil-targetlab.example
2013-11-29 15:55:00	POS-01	SSH Login	10.0.6.41	n/a	Login successful (possible credential reuse)
2013-11-29 16:00:00	LSASS-BOX	Process Memory Read	10.0.9.215	blackpos-lab.bin / SHA256: 928e13cd34af7245	Credential pattern found
2013-11-29 16:05:00	VPN-01	LSASS Dump Detected	10.0.2.124	lsass.dmp / SHA256: 111134e298d34d3e	Possible credential exfil from memory
2013-11-29 16:10:00	WORKSTATION-12	Large POST to external	10.0.2.161	cards-20131129_part1.csv / SHA256: 110484162d8f2a8c	Outbound to ftp-exfil-targetlab.example
2013-11-29 16:15:00	STAGE-01	Large POST to external	10.0.10.169	cards-20131129_part1.csv / SHA256:	Outbound to ftp-exfil-

				2f8c4bfca67590ad	targetlab.example
2013-11-29 16:20:00	ADMIN-01	FTP Upload Attempt	10.0.4.165	cards-20131129_part3.csv / SHA256: 842334f65f9079b5	Outbound to ftp-exfil-targetlab.example
2013-11-29 16:25:00	DB-01	Suspicious Process Spawn	10.0.10.217	proc: unknown_exec / SHA256: 65ee7734a85a03b7	Spawned by user 'svc_hvac'
2013-11-29 16:30:00	STAGE-01	FTP Upload Attempt	10.0.9.179	cards-20131129_part2.csv / SHA256: 6b6973dcf8cd4b02	Outbound to ftp-exfil-targetlab.example
2013-11-29 16:35:00	POS-01	SQL Dump	10.0.2.21	db-dump-20131129.sql / SHA256: 1a05d69b723c4c93	Sensitive data exported
2013-11-29 16:40:00	POS-01	Process Memory Read	10.0.4.186	blackpos-lab.bin / SHA256: 632528ddc08195bb	Credential pattern found
2013-11-29 16:45:00	WEB-01	Service Installed	10.0.10.100	service: backdoor_svc	Service started at boot
2013-11-29 16:50:00	STAGE-01	Service Installed	10.0.7.86	service: backdoor_svc	Service started at boot
2013-11-29 16:55:00	WORKSTATION-12	SQL Dump	10.0.6.27	db-dump-20131129.sql / SHA256: d870d52a4a1afe62	Sensitive data exported
2013-11-29 17:00:00	DB-01	Suspicious Process Spawn	10.0.3.11	proc: unknown_exec / SHA256: 3ad51277bc207f81	Spawned by user 'svc_hvac'

2013-11-29 17:05:00	LSASS-BOX	SSH Login	10.0.5.225	n/a	Login successful (possible credential reuse)
2013-11-29 17:10:00	STAGE-01	Config File Read	10.0.6.115	config.ini	Credentials found in config
2013-11-29 17:15:00	STAGE-01	Config File Read	10.0.2.211	config.ini	Credentials found in config
2013-11-29 17:20:00	ADMIN-01	Process Memory Read	10.0.4.108	blackpos-lab.bin / SHA256: ca25ef44c184bb56	Credential pattern found
2013-11-29 17:25:00	POS-01	Scheduled Task Creation	10.0.3.139	task: persist_worker	Persistence scheduled
2013-11-29 17:30:00	DB-01	Config File Read	10.0.9.60	config.ini	Credentials found in config
2013-11-29 17:35:00	DB-01	Scheduled Task Creation	10.0.2.55	task: persist_worker	Persistence scheduled
2013-11-29 17:40:00	STAGE-01	SQL Dump	10.0.1.138	db-dump-20131129.sql / SHA256: 81363fd4e9606ad8	Sensitive data exported
2013-11-29 17:45:00	VPN-01	Suspicious Process Spawn	10.0.7.13	proc: unknown_exec / SHA256: ce14fb490fc3d9ed	Spawned by user 'svc_hvac'
2013-11-29 17:50:00	ADMIN-01	LSASS Dump Detected	10.0.6.43	lsass.dmp / SHA256: 6569453d4aa21d34	Possible credential exfil from memory
2013-11-29 17:55:00	VPN-01	Process Memory Read	10.0.8.163	blackpos-lab.bin / SHA256: b1ab4dafd469b15d	Credential pattern found

2013-11-29 18:00:00	PROXY-01	Large POST to external	10.0.6.47	cards-20131129_part5.csv / SHA256: c4196950302f44e0	Outbound to ftp-exfil-targetlab.example
2013-11-29 18:05:00	WORKSTATION-12	Service Installed	10.0.2.30	service: backdoor_svc	Service started at boot
2013-11-29 18:10:00	VPN-01	Large POST to external	10.0.2.165	cards-20131129_part1.csv / SHA256: cc0873a374d47a46	Outbound to ftp-exfil-targetlab.example
2013-11-29 18:15:00	POS-01	Config File Read	10.0.9.99	config.ini	Credentials found in config
2013-11-29 18:20:00	ADMIN-01	LSASS Dump Detected	10.0.4.200	lsass.dmp / SHA256: 3e54fd25802542db	Possible credential exfil from memory
2013-11-29 18:25:00	POS-02	Process Memory Read	10.0.5.215	blackpos-lab.bin / SHA256: 4d245ca39b8d46fc	Credential pattern found
2013-11-29 18:30:00	LSASS-BOX	Scheduled Task Creation	10.0.9.250	task: persist_worker	Persistence scheduled
2013-11-29 18:35:00	WORKSTATION-12	Scheduled Task Creation	10.0.10.225	task: persist_worker	Persistence scheduled
2013-11-29 18:40:00	POS-01	LSASS Dump Detected	10.0.5.77	lsass.dmp / SHA256: 8145218b75e3e85a	Possible credential exfil from memory
2013-11-29 18:45:00	ADMIN-01	Suspicious Process Spawn	10.0.5.107	proc: unknown_exec / SHA256: 40e5ba94438b7e4a	Spawned by user 'svc_hvac'
2013-11-29 18:50:00	STAGE-01	Suspicious Process Spawn	10.0.7.38	proc: unknown_exec / SHA256: d6eb1d9665cb9108	Spawned by user 'svc_hvac'

2013-11-29 18:55:00	STAGE-01	Process Memory Read	10.0.9.187	blackpos-lab.bin / SHA256: 4f606210092eec6f	Credential pattern found
2013-11-29 19:00:00	WORKSTATION-12	SQL Dump	10.0.6.116	db-dump-20131129.sql / SHA256: f0989cb9998b198d	Sensitive data exported
2013-11-29 19:05:00	STAGE-01	FTP Upload Attempt	10.0.7.213	cards-20131129_part2.csv / SHA256: 7160c1f013e2994a	Outbound to ftp-exfil-targetlab.example
2013-11-29 19:10:00	DB-01	SSH Login	10.0.5.33	n/a	Login successful (possible credential reuse)
2013-11-29 19:15:00	STAGE-01	Suspicious Process Spawn	10.0.4.70	proc: unknown_exec / SHA256: 2079ecc29900d121	Spawned by user 'svc_hvac'
2013-11-29 19:20:00	ADMIN-01	Large POST to external	10.0.10.89	cards-20131129_part2.csv / SHA256: 9b953ffd5bf3bc16	Outbound to ftp-exfil-targetlab.example
2013-11-29 19:25:00	POS-02	Scheduled Task Creation	10.0.4.220	task: persist_worker	Persistence scheduled
2013-11-29 19:30:00	POS-01	LSASS Dump Detected	10.0.10.110	lsass.dmp / SHA256: f305109b0d0e1513	Possible credential exfil from memory
2013-11-29 19:35:00	PROXY-01	Large POST to external	10.0.4.252	cards-20131129_part6.csv / SHA256: bf6e8c3e5357c30f	Outbound to ftp-exfil-targetlab.example
2013-11-29 19:40:00	WORKSTATION-12	Suspicious	10.0.9.112	proc: unknown_exec / SHA256:	Spawned by user 'svc_hvac'

		Process Spawn		ef7fbc5ac20c4b47	
2013-11-29 19:45:00	LSASS-BOX	LSASS Dump Detected	10.0.10.73	lsass.dmp / SHA256: 2de904cf75fd589a	Possible credential exfil from memory
2013-11-29 19:50:00	PROXY-01	Process Memory Read	10.0.8.83	blackpos-lab.bin / SHA256: 30848b2006bf8183	Credential pattern found
2013-11-29 19:55:00	POS-02	FTP Upload Attempt	10.0.6.108	cards-20131129_part6.csv / SHA256: 5f707ce3c67177d6	Outbound to ftp-exfil-targetlab.example
2013-11-29 20:00:00	STAGE-01	LSASS Dump Detected	10.0.6.31	lsass.dmp / SHA256: 5a50e6ea7f586738	Possible credential exfil from memory
2013-11-29 20:05:00	STAGE-01	Large POST to external	10.0.4.117	cards-20131129_part1.csv / SHA256: d25c9c748a29c06c	Outbound to ftp-exfil-targetlab.example
2013-11-29 20:10:00	VPN-01	LSASS Dump Detected	10.0.7.179	lsass.dmp / SHA256: de68c9046c1372b4	Possible credential exfil from memory
2013-11-29 20:15:00	VPN-01	SQL Dump	10.0.6.215	db-dump-20131129.sql / SHA256: bbce0fd8fae81289	Sensitive data exported
2013-11-29 20:20:00	STAGE-01	FTP Upload Attempt	10.0.3.170	cards-20131129_part9.csv / SHA256: 01df0fb935363796	Outbound to ftp-exfil-targetlab.example
2013-11-29 20:25:00	PROXY-01	SQL Dump	10.0.8.89	db-dump-20131129.sql / SHA256: a2f34fbdc5aed325	Sensitive data exported

2013-11-29 20:30:00	ADMIN-01	Scheduled Task Creation	10.0.2.135	task: persist_worker	Persistence scheduled
2013-11-29 20:35:00	POS-02	LSASS Dump Detected	10.0.3.82	lsass.dmp / SHA256: 7e66d3dd7f3b9f20	Possible credential exfil from memory
2013-11-29 20:40:00	POS-01	Process Memory Read	10.0.8.249	blackpos-lab.bin / SHA256: 1cc9fa732a42c014	Credential pattern found
2013-11-29 20:45:00	POS-01	Suspicious Process Spawn	10.0.4.94	proc: unknown_exec / SHA256: 20cb34e7883a79dc	Spawned by user 'svc_hvac'
2013-11-29 20:50:00	LSASS-BOX	Service Installed	10.0.1.27	service: backdoor_svc	Service started at boot
2013-11-29 20:55:00	POS-01	SQL Dump	10.0.5.23	db-dump-20131129.sql / SHA256: a6b8d8fc4ab89bab	Sensitive data exported
2013-11-29 21:00:00	DB-01	Service Installed	10.0.7.35	service: backdoor_svc	Service started at boot
2013-11-29 21:05:00	STAGE-01	FTP Upload Attempt	10.0.8.82	cards-20131129_part5.csv / SHA256: a46d359a7adcdb61	Outbound to ftp-exfil-targetlab.example
2013-11-29 21:10:00	PROXY-01	Service Installed	10.0.7.123	service: backdoor_svc	Service started at boot
2013-11-29 21:15:00	DB-01	Scheduled Task Creation	10.0.5.20	task: persist_worker	Persistence scheduled
2013-11-29 21:20:00	ADMIN-01	Config File Read	10.0.2.50	config.ini	Credentials found in config
2013-11-29 21:25:00	WORKSTATION-12	Suspicious	10.0.4.107	proc: unknown_exec / SHA256:	Spawned by user 'svc_hvac'

		Process Spawn		2c997e95134de801	
2013-11-29 21:30:00	LSASS-BOX	Scheduled Task Creation	10.0.5.36	task: persist_worker	Persistence scheduled
2013-11-29 21:35:00	WORKSTATION-12	Scheduled Task Creation	10.0.7.166	task: persist_worker	Persistence scheduled
2013-11-29 21:40:00	LSASS-BOX	Process Memory Read	10.0.4.138	blackpos-lab.bin / SHA256: 35601431cedc4a3a	Credential pattern found
2013-11-29 21:45:00	LSASS-BOX	SQL Dump	10.0.7.38	db-dump-20131129.sql / SHA256: 0d6b2f9d90cb0b38	Sensitive data exported
2013-11-29 21:50:00	VPN-01	Process Memory Read	10.0.5.245	blackpos-lab.bin / SHA256: 3f3e4dafb4993e67	Credential pattern found
2013-11-29 21:55:00	DB-01	SQL Dump	10.0.3.150	db-dump-20131129.sql / SHA256: e451c6f9d9488bae	Sensitive data exported
2013-11-29 22:00:00	LSASS-BOX	Scheduled Task Creation	10.0.8.139	task: persist_worker	Persistence scheduled
2013-11-29 22:05:00	POS-01	SSH Login	10.0.9.240	n/a	Login successful (possible credential reuse)
2013-11-29 22:10:00	DB-01	Config File Read	10.0.5.109	config.ini	Credentials found in config
2013-11-29 22:15:00	POS-01	Config File Read	10.0.10.204	config.ini	Credentials found in config
2013-11-29 22:20:00	STAGE-01	Suspicious Process Spawn	10.0.10.17	proc: unknown_exec / SHA256:	Spawned by user 'svc_hvac'

				59f82b34988e94dd	
2013-11-29 22:25:00	POS-01	Suspicious Process Spawn	10.0.7.135	proc: unknown_exec / SHA256: 8fa8a4f7533d2377	Spawned by user 'svc_hvac'
2013-11-29 22:30:00	POS-02	LSASS Dump Detected	10.0.9.195	lsass.dmp / SHA256: 292eef2d19b786b9	Possible credential exfil from memory
2013-11-29 22:35:00	VPN-01	Service Installed	10.0.4.58	service: backdoor_svc	Service started at boot
2013-11-29 22:40:00	POS-01	Config File Read	10.0.7.99	config.ini	Credentials found in config
2013-11-29 22:45:00	WORKSTATION-12	FTP Upload Attempt	10.0.2.191	cards-20131129_part9.csv / SHA256: dac3b27bd0cecda2	Outbound to ftp-exfil-targetlab.example
2013-11-29 22:50:00	DB-01	Config File Read	10.0.9.215	config.ini	Credentials found in config
2013-11-29 22:55:00	WEB-01	LSASS Dump Detected	10.0.10.184	lsass.dmp / SHA256: 761cfe9de6c1f2b2	Possible credential exfil from memory
2013-11-29 23:00:00	DB-01	SQL Dump	10.0.7.49	db-dump-20131129.sql / SHA256: d9c4371d04ea3696	Sensitive data exported
2013-11-29 23:05:00	ADMIN-01	FTP Upload Attempt	10.0.1.253	cards-20131129_part6.csv / SHA256: b7b91e61bdf1c67e	Outbound to ftp-exfil-targetlab.example
2013-11-29 23:10:00	POS-02	FTP Upload Attempt	10.0.6.50	cards-20131129_part4.csv / SHA256: c5847f3ab670ae6f	Outbound to ftp-exfil-targetlab.example

2013-11-29 23:15:00	WORKSTATION-12	Service Installed	10.0.5.27	service: backdoor_svc	Service started at boot
2013-11-29 23:20:00	POS-02	LSASS Dump Detected	10.0.7.85	lsass.dmp / SHA256: 64f63ce53690375e	Possible credential exfil from memory
2013-11-29 23:25:00	PROXY-01	Scheduled Task Creation	10.0.1.222	task: persist_worker	Persistence scheduled
2013-11-29 23:30:00	VPN-01	SSH Login	10.0.6.198	n/a	Login successful (possible credential reuse)
2013-11-29 23:35:00	VPN-01	SQL Dump	10.0.1.37	db-dump-20131129.sql / SHA256: bab203e457e26192	Sensitive data exported
2013-11-29 23:40:00	POS-01	FTP Upload Attempt	10.0.7.254	cards-20131129_part3.csv / SHA256: 62583c52cbffb0f6	Outbound to ftp-exfil-targetlab.example
2013-11-29 23:45:00	PROXY-01	Scheduled Task Creation	10.0.2.230	task: persist_worker	Persistence scheduled
2013-11-29 23:50:00	WORKSTATION-12	Large POST to external	10.0.9.78	cards-20131129_part10.csv / SHA256: 858109f8d8c4ebf7	Outbound to ftp-exfil-targetlab.example
2013-11-29 23:55:00	DB-01	SQL Dump	10.0.4.32	db-dump-20131129.sql / SHA256: 58a332dd1c6493e3	Sensitive data exported
2013-11-30 00:00:00	PROXY-01	FTP Upload Attempt	10.0.7.217	cards-20131129_part6.csv / SHA256: 521ffb2bd0e9b31b	Outbound to ftp-exfil-targetlab.example

2013-11-30 00:05:00	POS-01	Config File Read	10.0.5.97	config.ini	Credentials found in config
2013-11-30 00:10:00	POS-02	SSH Login	10.0.4.76	n/a	Login successful (possible credential reuse)
2013-11-30 00:15:00	POS-01	Config File Read	10.0.3.156	config.ini	Credentials found in config
2013-11-30 00:20:00	WEB-01	Large POST to external	10.0.7.115	cards-20131129_part5.csv / SHA256: df97d92dd82d7160	Outbound to ftp-exfil-targetlab.example
2013-11-30 00:25:00	WORKSTATION-12	Scheduled Task Creation	10.0.10.215	task: persist_worker	Persistence scheduled
2013-11-30 00:30:00	LSASS-BOX	Suspicious Process Spawn	10.0.8.254	proc: unknown_exec / SHA256: 9c3e6af6f6180c64	Spawned by user 'svc_hvac'
2013-11-30 00:35:00	WORKSTATION-12	LSASS Dump Detected	10.0.8.90	lsass.dmp / SHA256: b70bd341ed530b35	Possible credential exfil from memory
2013-11-30 00:40:00	DB-01	LSASS Dump Detected	10.0.2.245	lsass.dmp / SHA256: be0cb2bc67eb9b43	Possible credential exfil from memory
2013-11-30 00:45:00	ADMIN-01	Large POST to external	10.0.9.170	cards-20131129_part1.csv / SHA256: 75e2a66da079b932	Outbound to ftp-exfil-targetlab.example
2013-11-30 00:50:00	LSASS-BOX	Large POST to external	10.0.7.56	cards-20131129_part8.csv / SHA256: d41b8af1da968ca2	Outbound to ftp-exfil-targetlab.example

2013-11-30 00:55:00	VPN-01	Service Installed	10.0.1.177	service: backdoor_svc	Service started at boot
2013-11-30 01:00:00	DB-01	Process Memory Read	10.0.10.229	blackpos-lab.bin / SHA256: f74636c9a6dec5bf	Credential pattern found
2013-11-30 01:05:00	LSASS-BOX	Service Installed	10.0.2.173	service: backdoor_svc	Service started at boot
2013-11-30 01:10:00	WEB-01	FTP Upload Attempt	10.0.4.1	cards-20131129_part1.csv / SHA256: 3dd47b1e739c1d1d	Outbound to ftp-exfil-targetlab.example
2013-11-30 01:15:00	WEB-01	LSASS Dump Detected	10.0.8.92	lsass.dmp / SHA256: 276dca0ba7eb16a0	Possible credential exfil from memory
2013-11-30 01:20:00	STAGE-01	SSH Login	10.0.4.195	n/a	Login successful (possible credential reuse)
2013-11-30 01:25:00	ADMIN-01	Service Installed	10.0.6.141	service: backdoor_svc	Service started at boot
2013-11-30 01:30:00	WEB-01	Suspicious Process Spawn	10.0.8.101	proc: unknown_exec / SHA256: 9e4d12485cb51e1b	Spawned by user 'svc_hvac'
2013-11-30 01:35:00	WORKSTATION-12	Scheduled Task Creation	10.0.9.193	task: persist_worker	Persistence scheduled
2013-11-30 01:40:00	POS-01	SSH Login	10.0.2.132	n/a	Login successful (possible credential reuse)
2013-11-30 01:45:00	WORKSTATION-12	SSH Login	10.0.4.231	n/a	Login successful (possible

					credential reuse)
2013-11-30 01:50:00	POS-02	SQL Dump	10.0.7.2	db-dump-20131129.sql / SHA256: 438b187127484d78	Sensitive data exported
2013-11-30 01:55:00	WORKSTATION-12	Service Installed	10.0.3.3	service: backdoor_svc	Service started at boot
2013-11-30 02:00:00	PROXY-01	Service Installed	10.0.2.109	service: backdoor_svc	Service started at boot
2013-11-30 02:05:00	DB-01	Large POST to external	10.0.6.213	cards-20131129_part10.csv / SHA256: 5001178f87560503	Outbound to ftp-exfil-targetlab.example
2013-11-30 02:10:00	DB-01	Process Memory Read	10.0.2.191	blackpos-lab.bin / SHA256: 24f6a192035f864d	Credential pattern found
2013-11-30 02:15:00	VPN-01	Scheduled Task Creation	10.0.8.17	task: persist_worker	Persistence scheduled
2013-11-30 02:20:00	ADMIN-01	FTP Upload Attempt	10.0.6.237	cards-20131129_part4.csv / SHA256: ce01ff4245df4466	Outbound to ftp-exfil-targetlab.example
2013-11-30 02:25:00	PROXY-01	SQL Dump	10.0.6.180	db-dump-20131129.sql / SHA256: e813f6085dc2b9db	Sensitive data exported
2013-11-30 02:30:00	WORKSTATION-12	Service Installed	10.0.3.37	service: backdoor_svc	Service started at boot
2013-11-30 02:35:00	VPN-01	Large POST to external	10.0.10.117	cards-20131129_part10.csv / SHA256: 400fb171f4347ee9	Outbound to ftp-exfil-targetlab.example

2013-11-30 02:40:00	WEB-01	Process Memory Read	10.0.7.133	blackpos-lab.bin / SHA256: e2bda3e62f3dec53	Credential pattern found
2013-11-30 02:45:00	LSASS-BOX	SQL Dump	10.0.3.105	db-dump-20131129.sql / SHA256: f9cb407a44838a45	Sensitive data exported
2013-11-30 02:50:00	POS-02	Suspicious Process Spawn	10.0.5.2	proc: unknown_exec / SHA256: be05a3d196aef8c8	Spawned by user 'svc_hvac'
2013-11-30 02:55:00	POS-02	Scheduled Task Creation	10.0.6.4	task: persist_worker	Persistence scheduled
2013-11-30 03:00:00	POS-02	Scheduled Task Creation	10.0.10.244	task: persist_worker	Persistence scheduled
2013-11-30 03:05:00	LSASS-BOX	SSH Login	10.0.5.151	n/a	Login successful (possible credential reuse)
2013-11-30 03:10:00	ADMIN-01	Config File Read	10.0.4.248	config.ini	Credentials found in config
2013-11-30 03:15:00	STAGE-01	Large POST to external	10.0.6.63	cards-20131129_part8.csv / SHA256: c0e80997db50435b	Outbound to ftp-exfil-targetlab.example
2013-11-30 03:20:00	STAGE-01	SSH Login	10.0.10.242	n/a	Login successful (possible credential reuse)
2013-11-30 03:25:00	STAGE-01	Process Memory Read	10.0.8.108	blackpos-lab.bin / SHA256: e869cc6ac1fc629c	Credential pattern found

2013-11-30 03:30:00	ADMIN-01	LSASS Dump Detected	10.0.4.160	lsass.dmp / SHA256: d81942dbed9c3a28	Possible credential exfil from memory
2013-11-30 03:35:00	VPN-01	Service Installed	10.0.2.58	service: backdoor_svc	Service started at boot
2013-11-30 03:40:00	VPN-01	Large POST to external	10.0.9.72	cards-20131129_part1.csv / SHA256: 2f25ef8892a937eb	Outbound to ftp-exfil-targetlab.example
2013-11-30 03:45:00	PROXY-01	SSH Login	10.0.5.114	n/a	Login successful (possible credential reuse)
2013-11-30 03:50:00	VPN-01	Scheduled Task Creation	10.0.6.240	task: persist_worker	Persistence scheduled
2013-11-30 03:55:00	WORKSTATION-12	Scheduled Task Creation	10.0.4.142	task: persist_worker	Persistence scheduled
2013-11-30 04:00:00	WEB-01	Large POST to external	10.0.5.249	cards-20131129_part1.csv / SHA256: 2adf79bd5922498a	Outbound to ftp-exfil-targetlab.example
2013-11-30 04:05:00	WORKSTATION-12	SQL Dump	10.0.4.55	db-dump-20131129.sql / SHA256: 4f1dff19803cf845	Sensitive data exported
2013-11-30 04:10:00	STAGE-01	Service Installed	10.0.2.76	service: backdoor_svc	Service started at boot
2013-11-30 04:15:00	POS-01	Process Memory Read	10.0.1.78	blackpos-lab.bin / SHA256: 236fa33cdfa4a93e	Credential pattern found
2013-11-30 04:20:00	PROXY-01	Suspicious Process Spawn	10.0.1.62	proc: unknown_exec / SHA256:	Spawned by user 'svc_hvac'

				60aae3a070e6c506	
2013-11-30 04:25:00	POS-01	FTP Upload Attempt	10.0.9.199	cards-20131129_part8.csv / SHA256: 2b7760c699c0703f	Outbound to ftp-exfil-targetlab.example
2013-11-30 04:30:00	STAGE-01	LSASS Dump Detected	10.0.10.11	lsass.dmp / SHA256: c7da6e58e2bf9bd0	Possible credential exfil from memory
2013-11-30 04:35:00	POS-02	Scheduled Task Creation	10.0.10.138	task: persist_worker	Persistence scheduled
2013-11-30 04:40:00	POS-02	LSASS Dump Detected	10.0.5.60	lsass.dmp / SHA256: dc6ecb759e708ca8	Possible credential exfil from memory
2013-11-30 04:45:00	WORKSTATION-12	Process Memory Read	10.0.8.99	blackpos-lab.bin / SHA256: 71bc5cec3daf47f5	Credential pattern found
2013-11-30 04:50:00	WORKSTATION-12	FTP Upload Attempt	10.0.1.147	cards-20131129_part1.csv / SHA256: e3977a9f3dc426ee	Outbound to ftp-exfil-targetlab.example
2013-11-30 04:55:00	POS-02	FTP Upload Attempt	10.0.9.181	cards-20131129_part2.csv / SHA256: 899dd387a124486e	Outbound to ftp-exfil-targetlab.example
2013-11-30 05:00:00	POS-01	SQL Dump	10.0.1.153	db-dump-20131129.sql / SHA256: c6bc506c73aa0f76	Sensitive data exported
2013-11-30 05:05:00	POS-02	Process Memory Read	10.0.4.94	blackpos-lab.bin / SHA256: 0e4c9632e0e4784c	Credential pattern found
2013-11-30 05:10:00	PROXY-01	Suspicious	10.0.9.101	proc: unknown_exec / SHA256:	Spawned by user 'svc_hvac'

		Process Spawn		99458975f221c769	
2013-11-30 05:15:00	WEB-01	Service Installed	10.0.6.66	service: backdoor_svc	Service started at boot
2013-11-30 05:20:00	WORKSTATION-12	FTP Upload Attempt	10.0.9.206	cards-20131129_part1.csv / SHA256: 84c714c3ea65f486	Outbound to ftp-exfil-targetlab.example
2013-11-30 05:25:00	WORKSTATION-12	Process Memory Read	10.0.9.117	blackpos-lab.bin / SHA256: 7d8ba738839f906c	Credential pattern found
2013-11-30 05:30:00	STAGE-01	Process Memory Read	10.0.9.27	blackpos-lab.bin / SHA256: cfe7e5b9a80458a9	Credential pattern found
2013-11-30 05:35:00	PROXY-01	Config File Read	10.0.6.89	config.ini	Credentials found in config
2013-11-30 05:40:00	VPN-01	FTP Upload Attempt	10.0.8.10	cards-20131129_part8.csv / SHA256: e249ea2439fb1bb1	Outbound to ftp-exfil-targetlab.example
2013-11-30 05:45:00	LSASS-BOX	Large POST to external	10.0.4.160	cards-20131129_part4.csv / SHA256: bfaf5cdef585a56e	Outbound to ftp-exfil-targetlab.example
2013-11-30 05:50:00	DB-01	Scheduled Task Creation	10.0.10.155	task: persist_worker	Persistence scheduled
2013-11-30 05:55:00	WORKSTATION-12	SSH Login	10.0.10.19	n/a	Login successful (possible credential reuse)
2013-11-30 06:00:00	WEB-01	Scheduled Task Creation	10.0.3.195	task: persist_worker	Persistence scheduled

2013-11-30 06:05:00	POS-02	SSH Login	10.0.9.154	n/a	Login successful (possible credential reuse)
2013-11-30 06:10:00	STAGE-01	Suspicious Process Spawn	10.0.7.122	proc: unknown_exec / SHA256: f88f46ab20ae03b5	Spawned by user 'svc_hvac'
2013-11-30 06:15:00	VPN-01	Suspicious Process Spawn	10.0.6.124	proc: unknown_exec / SHA256: c62af96724fac63b	Spawned by user 'svc_hvac'
2013-11-30 06:20:00	DB-01	Service Installed	10.0.5.148	service: backdoor_svc	Service started at boot
2013-11-30 06:25:00	POS-01	LSASS Dump Detected	10.0.4.163	lsass.dmp / SHA256: 42048aa974840765	Possible credential exfil from memory
2013-11-30 06:30:00	PROXY-01	Process Memory Read	10.0.9.212	blackpos-lab.bin / SHA256: 5c2f395426b296ec	Credential pattern found
2013-11-30 06:35:00	PROXY-01	Large POST to external	10.0.8.73	cards-20131129_part4.csv / SHA256: b844a46ef0393616	Outbound to ftp-exfil-targetlab.example
2013-11-30 06:40:00	LSASS-BOX	Process Memory Read	10.0.7.134	blackpos-lab.bin / SHA256: 19cb008c900a8122	Credential pattern found
2013-11-30 06:45:00	STAGE-01	SQL Dump	10.0.5.90	db-dump-20131129.sql / SHA256: a5d4c8e7c9a0eb7f	Sensitive data exported
2013-11-30 06:50:00	WORKSTATION-12	Scheduled Task Creation	10.0.3.201	task: persist_worker	Persistence scheduled

2013-11-30 06:55:00	ADMIN-01	Process Memory Read	10.0.3.136	blackpos-lab.bin / SHA256: c0652ae67d0ef924	Credential pattern found
2013-11-30 07:00:00	STAGE-01	Service Installed	10.0.4.94	service: backdoor_svc	Service started at boot
2013-11-30 07:05:00	DB-01	FTP Upload Attempt	10.0.1.91	cards-20131129_part1.csv / SHA256: 06cf0b882ef6dffa	Outbound to ftp-exfil-targetlab.example
2013-11-30 07:10:00	DB-01	SQL Dump	10.0.7.241	db-dump-20131129.sql / SHA256: b5b5d2863976af7a	Sensitive data exported
2013-11-30 07:15:00	POS-01	Service Installed	10.0.4.81	service: backdoor_svc	Service started at boot
2013-11-30 07:20:00	WEB-01	LSASS Dump Detected	10.0.6.127	lsass.dmp / SHA256: e86ff55df7e8d24d	Possible credential exfil from memory
2013-11-30 07:25:00	VPN-01	SSH Login	10.0.5.22	n/a	Login successful (possible credential reuse)
2013-11-30 07:30:00	WEB-01	FTP Upload Attempt	10.0.10.216	cards-20131129_part7.csv / SHA256: 92c2315b8e64ebfb	Outbound to ftp-exfil-targetlab.example
2013-11-30 07:35:00	POS-01	Scheduled Task Creation	10.0.5.122	task: persist_worker	Persistence scheduled
2013-11-30 07:40:00	DB-01	LSASS Dump Detected	10.0.3.173	lsass.dmp / SHA256: 1c00cb07f6cdc304	Possible credential exfil from memory
2013-11-30 07:45:00	WEB-01	Process Memory Read	10.0.5.116	blackpos-lab.bin / SHA256:	Credential pattern found

				0e3fd56f5d59fe5c	
2013-11-30 07:50:00	WORKSTATION-12	Suspicious Process Spawn	10.0.2.253	proc: unknown_exec / SHA256: a284aa86f4c2da34	Spawned by user 'svc_hvac'
2013-11-30 07:55:00	ADMIN-01	Config File Read	10.0.6.117	config.ini	Credentials found in config
2013-11-30 08:00:00	WEB-01	SQL Dump	10.0.6.253	db-dump-20131129.sql / SHA256: ae3a5a8ab3bf8448	Sensitive data exported
2013-11-30 08:05:00	PROXY-01	FTP Upload Attempt	10.0.1.17	cards-20131129_part2.csv / SHA256: b43c3900be5f5f50	Outbound to ftp-exfil-targetlab.example
2013-11-30 08:10:00	VPN-01	LSASS Dump Detected	10.0.3.251	lsass.dmp / SHA256: b68e9e59e0240edc	Possible credential exfil from memory
2013-11-30 08:15:00	PROXY-01	FTP Upload Attempt	10.0.8.239	cards-20131129_part5.csv / SHA256: 338d2f32d1d3a071	Outbound to ftp-exfil-targetlab.example
2013-11-30 08:20:00	STAGE-01	Process Memory Read	10.0.1.170	blackpos-lab.bin / SHA256: 722efe12b0b810a8	Credential pattern found
2013-11-30 08:25:00	PROXY-01	Large POST to external	10.0.1.107	cards-20131129_part1.csv / SHA256: 97bcacd1078ebe26	Outbound to ftp-exfil-targetlab.example
2013-11-30 08:30:00	POS-02	Suspicious Process Spawn	10.0.1.17	proc: unknown_exec / SHA256: 490f82df73a8eead	Spawned by user 'svc_hvac'

2013-11-30 08:35:00	POS-02	LSASS Dump Detected	10.0.3.58	lsass.dmp / SHA256: a10d1426dcbb25b2	Possible credential exfil from memory
2013-11-30 08:40:00	LSASS-BOX	Large POST to external	10.0.7.201	cards-20131129_part9.csv / SHA256: 865b2dd49c9253b2	Outbound to ftp-exfil-targetlab.example
2013-11-30 08:45:00	LSASS-BOX	Large POST to external	10.0.1.138	cards-20131129_part2.csv / SHA256: e7149c9aea07d4f8	Outbound to ftp-exfil-targetlab.example
2013-11-30 08:50:00	PROXY-01	Config File Read	10.0.8.209	config.ini	Credentials found in config
2013-11-30 08:55:00	POS-01	Scheduled Task Creation	10.0.5.198	task: persist_worker	Persistence scheduled
2013-11-30 09:00:00	VPN-01	FTP Upload Attempt	10.0.7.14	cards-20131129_part5.csv / SHA256: b13ccbd23b0894a3	Outbound to ftp-exfil-targetlab.example
2013-11-30 09:05:00	WORKSTATION-12	Suspicious Process Spawn	10.0.5.168	proc: unknown_exec / SHA256: 9a73dff0d8ef5fa0	Spawned by user 'svc_hvac'
2013-11-30 09:10:00	POS-02	Large POST to external	10.0.8.116	cards-20131129_part4.csv / SHA256: ce02838f65efe817	Outbound to ftp-exfil-targetlab.example
2013-11-30 09:15:00	POS-02	FTP Upload Attempt	10.0.9.104	cards-20131129_part9.csv / SHA256: a24e1365964acdce	Outbound to ftp-exfil-targetlab.example

Lưu ý:
- Các dữ liệu, hash và domain trong tài liệu này đều đã được giả hóa cho mục đích đào tạo.
- Không bao gồm mã độc thật; chỉ mô phỏng hành vi để phục vụ lab và phân tích.

Tài liệu tham khảo (gợi ý):
- Báo cáo điều tra vụ Target Breach (2013)
- Bài viết phân tích BlackPOS / memory-scraper
- MITRE ATT&CK: T1003 Credential Dumping